DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 through 164

RIN 0991–AB08

Standards for Privacy of Individually Identifiable Health Information

AGENCY: Office of the Assistant Secretary for Planning and Evaluation, DHHS.

ACTION: Proposed rule.

SUMMARY: This rule proposes standards to protect the privacy of individually identifiable health information maintained or transmitted in connection with certain administrative and financial transactions. The rules proposed below, which would apply to health plans, health care clearinghouses, and certain health care providers, propose standards with respect to the rights individuals who are the subject of this information should have, procedures for the exercise of those rights, and the authorized and required uses and disclosures of this information.

The use of these standards would improve the efficiency and effectiveness of public and private health programs and health care services by providing enhanced protections for individually identifiable health information. These protections would begin to address growing public concerns that advances in electronic technology in the health care industry are resulting, or may result, in a substantial erosion of the privacy surrounding individually identifiable health information maintained by health care providers, health plans and their administrative contractors. This rule would implement the privacy requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996.

DATES: Comments will be considered if received as provided below, no later than 5 p.m. on January 3, 2000.

ADDRESSES: Submit electronic comments at the following web site: http://aspe.hhs.gov/admnsimp/.

Mail comments (1 original, 3 copies, and, if possible, a floppy disk) to the following address: U.S. Department of Health and Human Services, Assistant Secretary for Planning and Evaluation, Attention: Privacy-P, Room G–322A, Hubert H. Humphrey Building, 200 Independence Avenue SW, Washington, DC 20201.

If you prefer, you may deliver your written comments (1 original, 3 copies, and, if possible, a floppy disk) to the following address: Room 442E, 200 Independence Avenue, SW, Washington, DC 20201.

See the **SUPPLEMENTARY INFORMATION** section for further information on comment procedures, availability of copies of this document and electronic access to this document.

FOR FURTHER INFORMATION CONTACT: Roxanne Gibson (202) 260–5083.

SUPPLEMENTARY INFORMATION: Comment procedures, availability of copies, and electronic access.

Comment procedures: All comments should include the full name, address and telephone number of the sender or a knowledgeable point of contact. Written comments should include 1 original and 3 copies. If possible, please send an electronic version of the comments on a 3½ inch DOS format floppy disk in Adobe Acrobat Portable Document Format (PDF) (preferred) HTML (preferred), ASCII text, or popular word processor format (Microsoft word, Corel WordPerfect).

Because of staffing and resource limitations, we cannot accept comments by electronic mail or facsimile (FAX) transmission, and all comments and content are to be limited to the 8.5 wide by 11.0 high vertical (also referred to as ‘‘portrait’’) page orientation. Additionally, it is requested that if identical/duplicate comment submissions are submitted both electronically and in paper form that each submission clearly indicate that it is a duplicate submission. In each comment, please specify the section of this proposed rule to which the comment applies.

Comments received in a timely fashion will be available for public inspection (by appointment), as they are received, generally beginning approximately three weeks after publication of a document in Room 442E of the Department's offices at 200 Independence Avenue, SW., Washington, DC 20201 on Monday through Friday of each week from 8:30 a.m. to 5 p.m. (phone: 202–260–5083).

After the close of the comment period, comments submitted electronically and written comments that we are technically able to convert will be posted on the Administrative Simplification web site (http://aspe.hhs.gov/admnsimp/).

Copies: To order copies of the **Federal Register** containing this document, send your request to: New Orders, Superintendent of Documents, PO Box 371954, Pittsburgh, PA 15250–7954. Specify the date of the issue requested and enclose a check or money order payable to the Superintendent of Documents, or enclose your Visa or Master Card number and expiration date. Credit card orders can also be placed by calling the order desk at (202) 512–1800 or by fax to (202) 512–2250. The cost for each copy is $8.00. As an alternative, you can view and photocopy the **Federal Register** document at most libraries designated as Federal Depository Libraries and at many other public and academic libraries throughout the country that receive the **Federal Register**.

Electronic Access: This document is available electronically at http://aspe.hhs.gov/admnsimp/ as well as at the web site of the Government Printing Office at http://www.access.gpo.gov/su_docs/aces/aces140.html.

I. Background

A. Need for Privacy Standards.

[*Please label comments about this section with the subject: ''Need for privacy standards''*]

The maintenance and exchange of individually identifiable health information is an integral component of the delivery of quality health care. In order to receive accurate and reliable diagnosis and treatment, patients must provide health care professionals with accurate, detailed information about their personal health, behavior, and other aspects of their lives. Health care providers, health plans and health care clearinghouses also rely on the provision of such information to accurately and promptly process claims for payment and for other administrative functions that directly affect a patient's ability to receive needed care, the quality of that care, and the efficiency with which it is delivered.

Individuals who provide information to health care providers and health plans increasingly are concerned about how their information is used within the health care system. Patients want to know that their sensitive information will be protected not only during the course of their treatment but also in the future as that information is maintained and/or transmitted within and outside of the health care system. Indeed, a Wall Street Journal/ABC poll on September 16, 1999 asked Americans what concerned them most in the coming century. ''Loss of personal privacy'' was the first or second concern of 29 percent of respondents. All other issues, such a terrorism, world war, and global warming had scores of 23 percent or less.

Efforts to provide legal protection against the inappropriate use of individually identifiable health information have been, to date, undertaken primarily by the States. States have adopted a number of laws designed to protect patients against the inappropriate use of health information. A recent survey of these laws indicates, however, that these protections are quite uneven and leave large gaps in their protection. See Health Privacy Project, ''The State of Health Privacy: An Uneven Terrain,'' Institute for Health Care Research and Policy, Georgetown University (July 1999) (http://www.healthprivacy.org).

A clear and consistent set of privacy standards would improve the effectiveness and the efficiency of the health care system. The number of entities who are maintaining and transmitting individually identifiable health information has increased significantly over the last 10 years. In addition, the rapid growth of integrated health care delivery systems requires greater use of integrated health information systems. The expanded use of electronic information has had clear benefits for patients and the health care system as a whole. Use of electronic information has helped to speed the delivery of effective care and the processing of billions of dollars worth of health care claims. Greater use of electronic data has also increased our ability to identify and treat those who are at risk for disease, conduct vital research, detect fraud and abuse, and measure and improve the quality of care delivered in the U.S.

The absence of national standards for the confidentiality of health information has, however, made the health care industry and the population in general uncomfortable about this primarily financially driven expansion in the use of electronic data. Many plans, providers, and clearinghouses have taken steps to safeguard the privacy of individually-identifiable health information. Yet they must currently rely on a patchwork of State laws and regulations that are incomplete and, at times, inconsistent. The establishment of a consistent foundation of privacy standards would, therefore, encourage the increased and proper use of electronic information while also protecting the very real needs of patients to safeguard their privacy.

The use of these standards will most clearly benefit patients who are, in increasing numbers, indicating that they are apprehensive about the use and potential use of their health information for inappropriate purposes. A national survey released in January 1999 indicated that one-fifth of Americans already believe that their personal health information has been used inappropriately. See California HealthCare Foundation, ''National Survey: Confidentiality of Medical Records,'' January 1999 (conducted by Princeton Survey Research Associates) (http://www.chcf.org). Of even greater concern, one-sixth of respondents indicated that they had taken some form of action to avoid the misuse of their information, including providing inaccurate information, frequently changing physicians, or avoiding care. The use of these standards will help to restore patient confidence in the health care system, providing benefits to both patients and those who serve them.

In order to administer their plans and provide services, private and public health plans, health care providers, and health care clearinghouses must assure their customers (such as patients, insurers, providers, and health plans) that the health care information they collect, maintain, use, or transmit will remain confidential. The protection of this information is particularly important where it is individually identifiable. Individuals have an important and legitimate interest in the privacy of their health information, and that interest is threatened where there is improper use or disclosure of the information. The risk of improper uses and disclosures has increased as the health care industry has begun to move from primarily paper-based information systems to systems that operate in various electronic forms. The ease of information collection, organization, retention, and exchange made possible by the advances in computer and other electronic technology afford many benefits to the health care industry and patients. At the same time, these advances have reduced or eliminated many of the logistical obstacles that previously served to protect the confidentiality of health information and the privacy interests of individuals.

Congress recognized the need for minimum national health care privacy standards to protect against inappropriate use of individually identifiable health information by passing the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191, which called for the enactment of a privacy statute within three years of the date of enactment. The legislation also called for the Secretary of Health and Human Services to develop and send to the Congress recommendations for protecting the confidentiality of health care information, which she did on September 11, 1997. The Congress further recognized the importance of such standards by providing the Secretary of Health and Human Services with authority to promulgate health privacy regulations in lieu of timely action by the Congress. The need for patient privacy protection also was recognized by the President's Advisory Commission on Consumer Protection and Quality in the Health Care Industry in its recommendations for a Consumer Bill of Rights and Responsibilities (November, 1997).

B. Statutory Background.

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

The Congress addressed the opportunities and challenges presented by the health care industry's increasing use of and reliance on electronic technology in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191, which was enacted on August 21, 1996. Sections 261 through 264 of HIPAA are known as the Administrative Simplification provisions. The major part of these Administrative Simplification provisions are found at section 262 of HIPAA, which enacted a new part C of title XI of the Social Security Act (hereinafter we refer to the Social Security Act as the ''Act'' and we refer to all other laws cited in this document by their names).

In section 262, Congress recognized and sought to facilitate the efficiencies and cost savings for the health care industry that the increasing use of electronic technology affords. Thus, section 262 directs HHS to issue standards to facilitate the electronic exchange of information with respect to financial and administrative transactions carried out by health plans, health care clearinghouses, and health care providers who transmit electronically in connection with such transactions. HHS proposed such standards in a series of Notices of Proposed Rulemaking (NPRM) published on May 7, 1998 (63 FR 25272 and 25320), and June 16, 1998 (63 FR 32784). At the same time, Congress recognized the challenges to the confidentiality of health information presented by the advances in electronic technology and communication. Section 262 thus also directs HHS to develop standards to protect the security, including the confidentiality and integrity, of such information. HHS issued an NPRM proposing security standards on August 12, 1998 (63 FR 43242).

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, a significant portion 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 provision. Although the requirement for the issuance of concomitant privacy standards remained as part of the bill passed by the House of Representatives, in conference the requirement for privacy standards was removed 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.

Part C of title XI consists of sections 1171 through 1179 of the Act. These sections define various terms and impose several requirements on HHS, health plans, health care clearinghouses, and health care providers who conduct the identified transactions electronically.

The first section, section 1171 of the Act, establishes definitions for purposes of part C of title XI for the following terms: code set, health care clearinghouse, health care provider, health information, health plan, individually identifiable health information, standard, and standard setting organization.

Section 1172 of the Act makes the standard adopted under part C applicable to: (1) Health plans, (2) health care clearinghouses, and (3) health care providers who transmit health information in electronic form in connection with transactions referred to in section 1173(a)(1) of the Act (hereinafter referred to as the ''covered entities''). Section 1172 also contains requirements concerning the adoption of standards, including the role of standard setting organizations and required consultations, summarized below.

Section 1173 of the Act requires the Secretary to adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically. Section 1173(a)(1) describes the transactions that are covered, which include the nine transactions listed in section 1173(a)(2) and other transactions determined appropriate by the Secretary. The remainder of section 1173 sets out requirements for the specific standards the Secretary is to adopt: unique health identifiers, code sets, security standards, electronic signatures, and transfer of information among health plans. Of particular relevance to this proposed rule is section 1173(d), the security standard provision. The security standard authority applies to both the transmission and the maintenance of health information and requires the entities described in section 1172(a) to maintain reasonable and appropriate safeguards to ensure the integrity and confidentiality of the information, protect against reasonably anticipated threats or hazards to the security or integrity of the information or unauthorized uses or disclosures of the information, and to ensure compliance with part C by the entity's officers and employees.

In section 1174 of the Act, the Secretary is required to establish standards for all of the above transactions, except claims attachments, by February 21, 1998. A proposed rule for most of the transactions was published in 1998 with the final rule expected by the end of 1999. The delay was caused by the deliberate consensus building process working with industry and the large number of comments received (about 17,000).

Generally, after a standard is established, it may not be changed during the first year after adoption except for changes that are necessary to permit compliance with the standard. Modifications to any of these standards may be made after the first year, but not more frequently than once every 12 months. The Secretary also must ensure that procedures exist for the routine maintenance, testing, enhancement and expansion of code sets and that there are crosswalks from prior versions.

Section 1175 of the Act prohibits health plans from refusing to process, or from delaying processing of, a transaction that is presented in standard format. It also establishes a timetable for compliance: each person to whom a standard or implementation specification applies is required to comply with the standard within 24 months (or 36 months for small health plans) of its adoption. A health plan or other entity may, of course, comply voluntarily before the effective date. The section also provides that compliance with modifications to standards or implementation specifications must be accomplished by a date designated by the Secretary, which date may not be earlier than 180 days from the notice of change.

Section 1176 of the Act establishes civil monetary penalties for violation of the provisions in part C of title XI of the Act, subject to several limitations. Penalties may not be more than $100 per person per violation and not more than $25,000 per person for violations of a single standard for a calendar year. The procedural provisions of section 1128A of the Act apply to actions taken to obtain civil monetary penalties under this section.

Section 1177 establishes penalties for any person that knowingly uses a unique health identifier, or obtains or discloses individually identifiable health information in violation of the part. The penalties include: (1) A fine of not more than $50,000 and/or imprisonment of not more than 1 year; (2) if the offense is ''under false pretenses,'' a fine of not more than $100,000 and/or imprisonment of not more than 5 years; and (3) if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than 10 years. We note that these penalties do not affect any other penalties that may be imposed by other federal programs.

Under section 1178 of the Act, the requirements of part C, as well as any standards or implementation specifications adopted thereunder, preempt contrary State law. There are three exceptions to this general rule of preemption: State laws that the Secretary determines are necessary for certain purposes set forth in the statute; State laws that the Secretary determines address controlled substances; and State laws relating to the privacy of individually identifiable health information that are contrary to and more stringent than the federal requirements. There also are certain areas of State law (generally relating to public health and oversight of health plans) that are explicitly carved out of the general rule of preemption and addressed separately.

Section 1179 of the Act makes the above provisions inapplicable to financial institutions or anyone acting on behalf of a financial institution when ''authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for a financial institution.'' Finally, as explained above, section 264 requires the Secretary to issue standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a)(1). Section 264 also contains a preemption provision that provides that contrary provisions of State laws that are more stringent than the federal standards, requirements, or implementation specifications will not be preempted.

C. Administrative Costs

Section 1172(b) of the Act provides that ''(a)ny standard adopted under this part (part C of title XI of the Act) shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.'' As is more fully discussed in the Regulatory Impact and Regulatory Flexibility analyses below, we recognize that the proposed privacy standards would entail substantial initial and ongoing administrative costs for entities subject to the rules. However, as the analyses also indicate, even if the rules proposed below are considered in isolation, they should produce administrative and other cost savings that should more than offset such costs on a national basis. It is also the case that the privacy standards, like the security standards authorized by section 1173(d) of the Act, are necessitated by the technological advances in information exchange that the remaining Administrative Simplification standards facilitate for the health care industry. The same technological advances that make possible enormous administrative cost savings for the industry as a whole have also made it possible to breach the security and privacy of health information on a scale that was previously inconceivable. The Congress recognized that adequate protection of the security and privacy of health information is a *sine qua non* of the increased efficiency of information exchange brought about by the electronic revolution, by enacting the security and privacy provisions of the law. Thus, even if the rules proposed below were to impose net costs, which we do not believe they do, they would still be ''consistent with'' the objective of reducing administrative costs for the health care system as a whole.

D. Consultations

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

The Congress explicitly required the Secretary to consult with specified groups in developing the standards under sections 262 and 264. Section 264(d) of HIPAA specifically requires the Secretary to consult with the National Committee on Vital and Health Statistics (NCVHS) and the Attorney General in carrying out her responsibilities under the section. Section 1172(b)(3) of the Act, which was enacted by section 262, requires that, in developing a standard under section 1172 for which no standard setting organization has already developed a standard, the Secretary must, before adopting the standard, consult with the National Uniform Billing Committee (NUBC), the National Uniform Claim Committee (NUCC), the Workgroup for Electronic Data Interchange (WEDI), and the American Dental Association (ADA). Section 1172(f) also requires the Secretary to rely on the recommendations of the NCVHS and consult with other appropriate federal and State agencies and private organizations.

We engaged in the required consultations including the Attorney General, NUBC, NUCC, WEDI and the ADA. We consulted with the NCVHS in developing the Recommendations, upon which this proposed rule is based. In addition we are continuing to consult with this committee by requesting the committee to review this proposed rule and provide comments, and recommendations will be taken into account in developing the final regulation. We consulted with representatives of the National Congress of American Indians, the National Indian Health Board, and the self governance tribes. We also met with representatives of the National Governors' Association, the National Conference of State Legislatures, the National Association of Public Health Statistics and Information Systems, and a number of other State organizations to discuss the framework for the proposed rule, issues of special interests to the States, and the process for providing comments on the proposed rule.

In addition to the required consultations, we met with numerous individuals, entities, and agencies regarding the regulation, with the goal of making these standards as compatible as possible with current business practices, while still enhancing privacy protection. Relevant federal agencies participated in an interagency working group, with additional representatives from all operating divisions and many staff offices of HHS. The following federal agencies and offices were represented on the interagency working group: the Department of Justice, the Department of Commerce, the Social Security Administration, the Department of Defense, the Department of Veterans Affairs, the Department of Labor, the Office of Personnel Management, and the Office of Management and Budget. The interagency working group developed the policies of the proposed rules set forth below.

E. Summary and Purpose of the Proposed Rule

[*Please label comments about this section with the subject: ''Summary and purpose''*]

The following outlines the provisions and operations of this proposed rule and is intended to provide a framework for the following preamble. A more detailed discussion of the authority, rationale, and implementation can be found in Section II of the preamble, Provisions of the Proposed Rule.

As described in more detail in preamble section I.B, above, the HIPAA requires the Secretary of HHS to promulgate a series of standards relating to the electronic exchange of health information. Collectively these are known as the Administrative Simplification provisions. In addition to those standards, the Secretary was required to develop and submit to the Congress recommendations for the privacy rights that an individual who is a subject of individually identifiable health information should have, the procedures that should be established for the exercise of such rights, and the uses and disclosures of such information that should be authorized.

On September 11, 1997, the Secretary presented to the Congress her Recommendations for protecting the ''Confidentiality of Individually-Identifiable Health Information'' (the ''Recommendations''), as required by section 264 (a) of HIPAA. In those Recommendations, the Secretary called for new federal legislation to create a national floor of standards that provide fundamental privacy rights for patients, and that define responsibilities for those who use and disclose identifiable health information.

The Recommendations elaborated on the components that should be included in privacy legislation. These components included new restrictions on the use and disclosure of health information, the establishment of new consumer rights, penalties for misuse of information, and redress for those harmed by misuse of their information. The Recommendations served, to the extent possible under the HIPAA legislative authority, as a template for the rules proposed below. They are available on the HHS website at http://aspe.hhs.gov/admnsimp/pvcrec.htm.

The Secretary's Recommendations set forth the a framework for federal privacy legislation. Such legislation should:

- Allow for the smooth flow of identifiable health information for treatment, payment, and related operations, and for specified additional purposes related to health care that are in the public interest.
- Prohibit the flow of identifiable information for any additional purposes, unless specifically and voluntarily authorized by the subject of the information.
- Put in place a set of fair information practices that allow individuals to know who is using their health information, and how it is being used.
- Establish fair information practices that allow individuals to obtain access to their records and request amendment of inaccurate information.
- Require persons who hold identifiable health information to safeguard that information from inappropriate use or disclosure.
- Hold those who use individually identifiable health information accountable for their handling of this information, and to provide legal recourse to persons harmed by misuse.

We believed then, and still believe, that there is an urgent need for legislation to establish comprehensive privacy standards for all those who pay and provide for health care, and those who receive information from them.

This proposed rule implements many of the policies set forth in the Recommendations. However, the HIPAA legislative authority is more limited in scope than the federal statute we recommend, and does not always permit us to propose the policies that we believe are optimal. Our major concerns with the scope of the HIPAA authority include the limited number of entities to whom the proposed rule would be applicable, and the absence of strong enforcement provisions and a private right of action for individuals whose privacy rights are violated.

The Recommendations call for legislation that applies to health care providers and payers who obtain identifiable health information from individuals and, significantly, to those who receive such information from providers and payers. The Recommendations follow health information from initial creation by a health plan or health care provider, through various uses and disclosures, and would establish protections at each step: ''We recommend that everyone in this chain of information handling be covered by the same rules.'' However, the HIPAA limits the application of our proposed rule to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions referred to in section 1173(a)(1) of the Act (the ''covered entities''). Unfortunately, this leaves many entities that receive, use and disclose protected health information outside of the system of protection that we propose to create.

In particular, the proposed regulation does not directly cover many of the persons who obtain identifiable health information from the covered entities. In this proposed rule we are, therefore, faced with creating new regulatory permissions for covered entities to disclose health information, but cannot directly put in place appropriate restrictions on how many likely recipients of such information may use and re-disclose such information. For example, the Secretary's Recommendations proposed that protected health information obtained by researchers not be further disclosed except for emergency circumstances, for a research project that meets certain conditions, and for oversight of research. In this proposed rule, however, we cannot impose such restrictions. Additional examples of persons who receive this information include workers compensation carriers, researchers, life insurance issuers, employers and marketing firms. We also do not have the authority to directly regulate many of the persons that covered entities hire to perform administrative, legal, accounting, and similar services on their behalf, and who would obtain health information in order to perform their duties. This inability to directly address the information practices of these groups leaves an important gap in the protections provided by the proposed rule.

In addition, only those providers who engage in the electronic administrative simplification transactions can be covered by this rule. Any provider who maintains a solely paper information system would not be subject to these privacy standards, thus leaving another gap in the system of protection we propose to create.

The need to match a regulation limited to a narrow range of covered entities with the reality of information sharing among a wide range of entities leads us to consider limiting the type or scope of the disclosures permitted under this regulation. The disclosures we propose to allow in this rule are, however, necessary for smooth operation of the health care system and for promoting key public goals such as research, public health, and law enforcement. Any limitation on such disclosures could do more harm than good.

Requirements to protect individually identifiable health information must be supported by real and significant penalties for violations. We recommend federal legislation that would include punishment for those who misuse personal health information and redress for people who are harmed by its misuse. We believe there should be criminal penalties (including fines and imprisonment) for obtaining health information under false pretenses, and for knowingly disclosing or using protected health information in violation of the federal privacy law. We also believe that there should be civil monetary penalties for other violations of the law and that any individual whose rights under the law have been violated, whether negligently or knowingly, should be permitted to bring an action for actual damages and equitable relief. Only if we put the force of law behind our rhetoric can we expect people to have confidence that their health information is protected, and ensure that those holding health information will take their responsibilities seriously.

In HIPAA, Congress did not provide such enforcement authority. There is no private right of action for individuals to enforce their rights, and we are concerned that the penalty structure does not reflect the importance of these privacy protections and the need to maintain individuals' trust in the system. For these and other reasons, we continue to call for federal legislation to ensure that privacy protection for health information will be strong and comprehensive.

1. Applicability

a. *Entities covered.* Under section 1172(a) of the Act, the provisions of this proposed rule apply to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions referred to in section 1173(a)(1) of the Act (the ''covered entities''). The terms health plan, health care provider, and health care clearinghouse are defined in proposed § 160.103.

As noted above, because we do not have the authority to apply these standards directly to any entity that is not a covered entity, the proposed rule does not directly cover many of the persons who obtain identifiable health information from the covered entities. Examples of persons who receive this information include contractors, third-party administrators, researchers, public health officials, life insurance issuers, employers and marketing firms. We would attempt to fill this gap in our legislative authority in part by requiring covered entities to apply many of the provisions of rule to the entities with whom they contract for administrative and other services. The proposed provision is outlined in more detail below in the discussion of business partners.

b. *Protected health information.* We propose to apply the requirements of this rule to the subset of individual identifiable health information which is maintained or transmitted by covered entities and which is or has been in electronic form. The provisions of the rule would apply to the information itself, referred to as protected health information in this rule, and not to the particular records in which the information is contained. Once information has been maintained or transmitted electronically by a covered entity, the protections would follow the information in whatever form, including paper records, in which it exists (while it is held by a covered entity).

We understand that our proposal would create a situation in which some health information would be protected while other similar information (e.g., health information contained in paper records that has not been maintained or transmitted electronically) would not be protected. We are concerned about the potential confusion that such a system might entail, but we believe that applying the provisions of the rule to information only in electronic form would result in no real protection for health care consumers. We have requested comment on whether we should extend the scope of the rule to all individually identifiable health information, including purely paper records, maintained by covered entities. Although we are concerned that extending our regulatory coverage to all records might be inconsistent with the intent of the provisions in the HIPAA, we believe that we do have the authority to do so and that there are sound rationale for providing a consistent level of protection to all individually identifiable health information held by covered entities.

2. General Rules

The purpose of our proposal is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by others. We are proposing to make the use and exchange of protected health information relatively easy for health care purposes, and more difficult for purposes other than health care.

Covered entities would be prohibited from using or disclosing protected health information except as provided in the proposed rule. Under the rule, covered entities could use or disclose protected health information with individual authorization, as provided in proposed § 164.508. Covered entities could use or disclose protected health information without authorization for treatment, payment and health care operations, as provided in § 164.506(a). (The terms ''treatment,'' ''payment'' and ''health care operations'' are defined in proposed § 164.504). Covered entities also would be permitted to use or disclose a patient's protected health information without authorization for specified public and public policy-related purposes, including public health, research, health oversight, law enforcement, and use by coroners, as provided in proposed § 164.510. Covered entities would be permitted to use and disclose protected health information when required to do so by other law, such as mandatory reporting under state law or pursuant to a search warrant.

Covered entities would be required by this rule to disclose protected health information for only two purposes: to permit individuals to inspect and copy protected health information about them, pursuant to proposed § 164.514, and for enforcement of this rule pursuant to proposed § 164.522.

Under our proposal, most uses and disclosures of an individual's protected health information would not require explicit authorization by the individual, but would be restricted by the provisions of the rule. As discussed in section II.C. of this preamble, we propose to substitute regulatory protections for the pro forma authorizations that are used today. The rules would create a sphere of privacy protection that includes covered entities who engage in treatment or payment, and the business partners they hire to assist them. While written consent for these activities would not be required, new restrictions on both internal uses and external disclosures would be put in place to protect the information.

Our proposal is based on the principle that a combination of strict limits on how plans and providers can use and disclose identifiable health information, adequate notice to patients about how such information will be used, and patients' rights to inspect, copy and amend protected health information about them, will provide patients with better privacy protection and more effective control over the dissemination of their information than alternative approaches to patient protection and control.

A central aspect of this proposal is the principle of ''minimum necessary'' disclosure. (See proposed § 164.506(a)). With certain exceptions, permitted uses and disclosures of protected health information would be restricted to the minimum amount of information necessary to accomplish the purpose for which the information is used or disclosed, taking into consideration practical and technological limitations (including the size and nature of the covered entity's business) and costs. While we recognize that there are legitimate uses of protected health information for which patient authorization should not be required, the privilege of this access carries with it an obligation to safeguard the information. Covered entities would be required to take steps to limit the amount of protected health information used or disclosed to the information necessary to meet the purpose of the use or disclosure. These policies could include limiting access to the information to a subset of employees who need to use the information in the course of their work, and limiting the amount of information disclosed from a record to the information needed by the recipient to fulfill the purpose of the disclosure.

We propose that individuals be able to request that a covered entity restrict the protected health information that results from that encounter (with the exception of encounters for emergency treatment) from further use or disclosure for treatment, payment, and health care operations. (See proposed § 164.506(c)). Covered entities would not be required to agree to restrictions requested by individuals; the rule would only enforce a restriction that has been agreed to by the covered entity and the individual.

Today's health care system is a complex business involving multiple individuals and organizations engaging in a variety of commercial relationships. An individual's privacy should not be compromised when a covered entity engages in such normal business relationships. To accomplish this result, the rule would, with narrow exceptions, require covered entities to ensure that the business partners with which they share protected health information understand—through contract requirements '' that they are subject to standards regarding use and disclosure of protected health information and agree to abide by such rules. (See proposed § 164.506(e)). Other than for purposes of treatment consultation or referral, we would require a contract to exist between the covered entity and the business partner that would, among other specified provisions, limit the business partner's uses and disclosures of protected health information to those permitted by the contract and would impose certain security, inspection and reporting requirements on the business partner.

We do not intend to interfere with business relationships in the health care industry, but rather to ensure that the privacy of the information shared in these relationships is protected. Business partners would not be permitted to use or disclose protected health information in ways that would not be permitted by the covered entity itself.

3. Scalability

The privacy standards would need to be implemented by all covered entities, from the smallest provider to the largest, multi-state health plan. For this reason, we propose the privacy principles and standards that covered entities must meet, but leave the detailed policies and procedures for meeting these standards to the discretion of each covered entity. We intend that implementation of these standards be flexible and scalable, to account for nature of each covered entity's business, as well as the covered entity's size and resources. A single approach to implementation of these requirements would be neither economically feasible nor effective in safeguarding health information privacy. Instead, we would require that each covered entity assess its own needs and devise and implement privacy policies appropriate to its size, its information practices, and its business requirements. Examples of how implementation of these standards are scalable are provided in the relevant sections of this preamble. (See, also, the discussion in preamble sections II.C. and III.)

4. Uses and Disclosures With Individual Authorization

The rule would require that covered entities have authorization from individuals before using or disclosing their protected health information for any purpose not otherwise recognized by this rule. In § 164.508, we propose rules for obtaining authorizations. Authorizations are needed in a wide array of circumstances. Entities not covered by this rule often want access to individually identifiable health information . For example, a potential employer may require health information as part of a background check for security purposes, or the patient may request a plan or provider to disclose information to obtain eligibility for disability benefits or to an attorney for use in a law suit. Covered entities may also seek such an authorization in order to use protected health information for a purpose not otherwise permitted under this rule. For example, a health plan may wish to use a person's records for developing a marketing strategy.

The proposed authorization requirements are intended to ensure that an individual's authorization is truly voluntary. We would prohibit covered entities from conditioning treatment or payment on the individual agreeing to disclose information for other purposes. We also would require authorizations to clearly and specifically describe the information to be disclosed. If an authorization is sought so that a covered entity may sell, barter, or otherwise exchange the information for purposes other than treatment, payment, or health care operations, the covered entity would have to disclose this fact on the authorization form. We would also require authorizations to be revocable. We do not seek to limit the purposes for which authorization of records disclosure may be sought, but rather to ensure that these authorizations are voluntary, fair, and enforceable.

While the provisions of this proposed rule are intended to make authorizations for treatment and payment purposes unnecessary, some States may continue to require them. This rule would not supersede such State requirements generally, but would impose a new requirement that such State-mandated authorizations must be physically separate from an authorization for other purposes described in this rule.

5. Uses and Disclosures for Treatment, Payment and Health Care Operations

Under this rule, covered entities with limited exceptions would be permitted to use and disclose protected health information without individual authorization for treatment and payment purposes, and for related purposes that we have defined as health care operations. (See § 164.506.) We would construe the terms ''treatment'' and ''payment'' broadly. In section II.B. of this preamble, we describe the types of activities that would be considered health care operations.

6. Permissible Uses and Disclosures for Purposes Other Than Treatment, Payment and Health Care Operations

Individually identifiable health information is needed to support certain national priority activities, such as reducing health care fraud, improving the quality of treatment through research, protecting the public health, and responding to emergency situations. In many cases, the need to obtain authorization for use of health information would create significant obstacles in efforts to fight crime, understand disease, and protect public health. We examined the many uses that the health professions, related industries, and the government make of health information and we are aware of the concerns of privacy and consumer advocates about these uses.

After balancing privacy and other social values, we are proposing rules that would permit use or disclosure of health information without individual authorization for the following national priority activities and activities that allow the health care system to operate smoothly:

- Oversight of the health care system
- Public health functions
- Research
- Judicial and administrative proceedings
- Law enforcement
- Emergency circumstances
- To provide information to next-of-kin
- For identification of the body of a deceased person, or the cause of death
- For government health data systems
- For facility patient directories
- To banks, to process health care payments and premiums
- For management of active duty military and other special classes of individuals

• Where other law requires such disclosure and no other category of permissible disclosures would allow the disclosure

The rule would specify conditions that would need to be met in order for the use or disclosure of protected health information to be permitted for each of these purposes. (See § 164.514) We have proposed conditions tailored to the need for each type of use or disclosure, and to the types of organizations involved in each such activity. These uses and disclosures, and the conditions under which they may occur, are discussed in section II. F of this preamble.

The uses and disclosures that would be permitted under proposed rule would be just that—permissible. Thus, for disclosures that are not compelled by other law, providers and payers would be free to disclose or not, according to their own policies and ethical principles. We propose these rules as a basic set of legal controls, but ethics and professional practice may dictate more guarded disclosure policies. At the same time, nothing in this rule would provide authority for a covered entity to restrict or refuse to make a disclosure mandated by other law.

7. Individual Rights

We are proposing to establish several basic rights for individuals with respect to their protected health information. We propose that individuals be able to obtain access to protected health information about them, which would include a right to inspect and obtain a copy of such information. See proposed § 164.514. The right of access would extend to an accounting of disclosures of the protected health information for purposes other than treatment, payment, and health care operations. See proposed § 164.515.

In § 164.512, we also propose that individuals have a right to receive a written notice of information practices from covered entities. While the primary purpose of this notice would be to inform individuals about the uses and disclosures that a covered entity would intend to make with the information, the notice also would serve to limit the activities of the covered entity—an otherwise lawful use or disclosure that does not appear in the entity's notice would not be permitted. The covered entity's uses and disclosures could be stated in broad terms, but an entity would not be able to make a use or disclosure that is not included in its notice. The covered entity could modify its notice at any time and apply revised practices to existing and new information held by the covered entity.

In addition, we propose that individuals have the right to request amendment or correction of protected health information that is inaccurate or incomplete. See proposed § 164.516. We are proposing procedural requirements and deadlines to implement each of these individual rights.

8. Administrative Requirements and Policy Development and Documentation

In our Recommendations, we call for a federal law that requires holders of identifiable health information to implement safeguards to protect it from inappropriate access, use or disclosure. No legislation or rule can effectively specify how to do this for every holder of health information. But federal rules can and should require those who hold identifiable health information to develop and implement basic administrative procedures to protect that information and protect the rights of the individual with respect to that information.

To accomplish this goal, we propose that covered entities be required to designate a privacy official, develop a privacy training program for employees, implement safeguards to protect health information from intentional or accidental misuse, provide some means for individuals to lodge complaints about the covered entity's information practices, and develop a system of sanctions for employees and business partners who violate the entity's policies or procedures. (See proposed § 164.518.). We also propose, in § 164.520, to require covered entities to maintain documentation of their policies and procedures for complying with the requirements of this proposed rule. The purpose of these requirements is to ensure that covered entities make explicit decisions about who would have access to protected health information, how that information would be used within the entity, and when that information would or would not be disclosed to other entities.

9. Preemption

The HIPAA provides that the rule promulgated by the Secretary may not preempt state laws that are in conflict with the regulatory requirements and that provide greater privacy protections. The HIPAA also provides that standards issued by the Secretary will not supercede certain other State laws, including: State laws relating to reporting of disease or injury, child abuse, birth or death, public health surveillance, or public health investigation or intervention; State regulatory reporting; State laws which the Secretary finds are necessary to prevent fraud and abuse, to ensure appropriate State regulation of insurance, for State reporting on health care delivery or costs, or for other purposes; or, State laws which the Secretary finds address controlled substances. These provisions are discussed in more detail in preamble section II.I.1.

This proposed rule also must be read in conjunction with other federal laws and regulations that address the use and disclosure of health information. These issues are discussed in preamble section II.I.2.

In general, the rule that we are proposing would create a federal floor of privacy protection, but would not supercede other applicable law that provide greater protection to the confidentiality of health information. In general, our rule would not make entities subject to a state laws to which they are not subject today.

10. Enforcement

The HIPAA grants the Secretary the authority to impose civil monetary penalties against covered entities which fail to comply with the requirements of this rule, and also establishes criminal penalties for certain wrongful disclosures of protected health information. The civil fines are capped at $25,000 for each calendar year for each provision that is violated. The criminal penalties are graduated, increasing if the offense is committed under false pretenses, or with intent to sell the information or reap other personal gain. The statute does not provide for a private right of action for individuals.

We propose to create a complaint system to permit individuals to make complaints to the Secretary about potential violations of this rule. We also propose that covered entities develop a process for receiving complaints from individuals about the entities' privacy practices. (See § 164.522.) Our intent would be to work with covered entities to achieve voluntary compliance with the proposed standards.

11. Conclusion

Although the promise of these proposed standards cannot become reality for many patients because of the gaps in our authority, we believe they would provide important new protections. By placing strict boundaries around the ways covered entities could use and disclose information, these rules would protect health information at its primary sources: health plans and health care providers. By requiring covered entities to inform patients about how their information is being used and shared, by requiring covered entities to provide access to that information, and by ensuring that authorizations would be truly voluntary, these rules would provide patients with important new tools for understanding and controlling information about them. By requiring covered entities to document their privacy practices, this rule would focus attention on the importance of privacy, and reduce the ways in which privacy is compromised through inattention or misuse.

With the Secretary's recommendations and these proposed rules, we are attempting to further two important goals: to allow the free flow of health information needed to provide and promote high quality health care, while assuring that individuals' health information is properly protected. We seek a balance that permits important uses of information privacy of people who seek care and healing. We believe our Recommendations find that balance, and have attempted to craft this proposed rule to strike that balance as well.

We continue to believe, however, that federal legislation is the best way to guarantee these protections. The HIPAA legislative authority does not allow full implementation of our recommended policies in this proposed rule. The legislation limits the entities that can be held responsible for their use of protected health information, and the ways in which the covered entities can be held accountable. For these and other reasons, we continue to call upon Congress to pass comprehensive federal privacy legislation. Publication of this proposed rule does not diminish our firm conviction that such legislation should be enacted as soon as possible.

II. Provisions of the Proposed Rule

We propose to establish a new subchapter C to title 45 of the Code of Federal Regulations. Although the rules proposed below would only establish two new parts (parts 160 and 164), we anticipate the new subchapter C will eventually contain three parts, part 160, 162, and 164, with parts 161 and 163 being reserved for future expansion, if needed. Part 160 will contain general requirements and provisions applicable to all of the regulations issued under sections 262 and 264 of Public Law 104–191 (the Administrative Simplification provisions of HIPAA). We anticipate that Part 162 will contain the Administrative Simplification regulations relating to transactions, code sets and identifiers. The new part 164 will encompass the rules relating to the security standards authorized by section 1173(d), the electronic signature standard authorized by section 1173(e), and the privacy rules proposed below.

The new part 164 will be composed of two subparts: subparts A and E, with B, C, and D being reserved. Subpart A will consist of general provisions and subpart E will consist of the final privacy rules. Because the new part 160 will apply to the privacy rules, as well as the other Administrative Simplification rules, it is set out below.

A. Applicability

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

The discussion below describes the entities and the information that would be subject to the proposed regulation.

1. Covered Entities

The standards in this proposed regulation would apply to all health plans, all health care clearinghouses, and all health care providers that transmit health information in an electronic form in connection with a standard transaction. In this proposed rule, these entities are referred to as ''covered entities.'' See definition at proposed § 160.103.

A health plan is defined by section 1171 to be an individual or group plan that provides for, or pays the cost of, medical care. The statute expressly includes a significant group of employee welfare benefit plans, state-regulated insurance plans, managed care plans, and essentially all government health plans, including Medicare, Medicaid, the veterans health care program, and plans participating in the Federal Employees Health Benefits Program. See discussion of the definition in section II.B.

A health care provider would be a provider of services as defined in section 1861(u) of the Act, 42 U.S.C. 1395x, a provider of medical or other health services as defined in section 1861(s) of the Act, and any other person who furnishes, bills or is paid for health care services or supplies in the normal course of business. See discussion of the definition in section II.B. Health care providers would be subject to the provisions of the rule if they transmit health information in electronic form in connection with a standard transaction. Standard transactions include claims and equivalent encounter information, eligibility and enrollment transactions, premium payments, claims attachments, and others. See proposed § 160.103. Health care providers who themselves do not directly conduct electronic transactions would become subject to the provisions of the proposed rule if another entity, such as a billing agent or hospital, transmits health information in electronic form in connection with a standard transaction on their behalf.

A health care clearinghouse would be a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. See section 1171(2) of the Act. For purposes of this rule, we would consider billing services, repricing companies, community health management information systems or community health information systems, ''value-added'' networks, switches and similar organizations to be health care clearinghouses for purposes of this part only if they actually perform the same functions as a health care clearinghouse. See discussion of the definition in section II.B.

2. Covered Information

We propose to apply the standards in this proposed regulation to individually identifiable health information that is or has been electronically transmitted or maintained by a covered entity, including such information when it is in non-electronic form (e.g., printed on paper) or discussed orally. In this proposed regulation, such information is referred to as ''protected health information.'' See discussion of the definition in section II.B. Under HIPAA, our authority to promulgate privacy standards extends to all individually identifiable health information, in any form, maintained or transmitted by a covered entity. For reasons discussed below, we are proposing to limit the application of the proposed standards to protected health information. Below we invite comment on whether we should apply the standards to a broader set of individually identifiable health information in the future.

Under the proposal, the standards apply to information, not to specific records. Thus, once protected health information is transmitted or maintained electronically, the protections afforded by this regulation would apply to the information in any form and continue to apply as the information is printed, discussed orally or otherwise changed in form. It would also apply to the original paper version of information that is at some point transmitted electronically. The authority for, and implications of, this scope are discussed in detail in this section, below.

This proposed regulation would not apply to information that has never been electronically maintained or transmitted by a covered entity.

a. *Legislative authority.* Under HIPAA, we have authority to promulgate a privacy standard that applies to all individually identifiable health information transmitted or maintained by a covered entity, including information in a non-electronic form. We recognize that there may be an expectation that we would apply privacy standards only to information that is electronically maintained and transmitted. Our prior proposals under HIPAA have addressed only electronically maintained and transmitted information. See Notices of Proposed Rulemaking (NPRM) published on May 7, 1998 (63 FR 25272 and 25320), June 16, 1998 (63 FR 32784), and the proposed security standards published on August 12, 1998 (63 FR 43242).

In considering the appropriate reach of the proposed privacy standards, however, we determined that limiting the standards to electronic information would not be consistent with the requirement in HIPAA for the Secretary to address privacy, confidentiality and security concerns relating to individually identifiable health information.

The HIPAA statute, taken as a whole, contemplates an information protection system that assures the privacy, confidentiality and integrity of health information. Two provisions in subtitle F of HIPAA address privacy and confidentiality concerns: section 264, titled ''Recommendations with Respect to Privacy of Certain Health Information'' and section 1173(d), titled ''Security Standards for Health Information.'' See 42 U.S.C. 1320d–1320d–8, enacted as sections 262 and 264 of HIPAA.

In enacting HIPAA, Congress recognized that the increased accessibility of health information made possible by the widespread and growing use of electronic media and the new federal mandate for increased standardization of data, requires enhanced privacy and confidentiality protections. The House Report links privacy and security concerns stating: ''The standards adopted would protect the privacy and confidentiality of health information. Health information is considered relatively ''safe'' today, not because it is secure, but because it is difficult to access. These standards improve access and establish strict privacy protections.'' House Report No. 496, 104th Cong., 2d. Sess., at 99.

Section 264(c) authorizes the Secretary to protect the privacy of individually identifiable health information transmitted in connection with the standard transactions. Section 1173(d) authorizes the Secretary to prescribe requirements that address the security, integrity, and confidentiality of health information maintained or transmitted, in any form or medium, by the covered entities.

Neither the privacy authority in section 264(c) nor the security authority in 1173(d) exclusively limit the scope of protection to electronic information. Section 264(c) of HIPAA requires the Secretary to issue a regulation setting privacy standards for individually identifiable health information ''transmitted in connection with the transactions described in section 1173(a).'' This statutory language is not on its face limited to electronic transmissions of individually identifiable health information, although electronic transmissions of such information are clearly within its scope. Moreover, the section requires the regulations to address ''at least'' the subjects of the Secretary's Recommendations, which focus on individually identifiable health information, without reference to whether the information is electronic or not.

The security provision also is not limited by its terms to electronically maintained information. Rather, section 1173(d) applies throughout to ''health information,'' a statutorily defined term that clearly covers information in both its electronic and non-electronic forms.

In HIPAA, when Congress intended to limit health information to its electronic form, it did so explicitly. Section 1172(a)(3) of the statute says that the standards apply to health plans and to health care providers who transmit health information *in electronic form* in connection with the standard transactions (emphasis added); by contrast, the section 1173(d) requirements for information maintained or transmitted are not similarly qualified.

Further support for the premise that the standards may reach information that is maintained or transmitted non-electronically is found within section 1173(d) itself. That section explicitly distinguishes within one subsection (§ 1173(d)(1)(A)) between ''record systems used to maintain health information'' and ''*computerized* record systems.'' Thus, the conclusion may be drawn that the record systems covered by the § 1173(d) security standards are intended to include record systems other than those that are exclusively electronic or ''computerized.''

Finally, the section that generally defines the HIPAA standard transactions, section 1173(a), is not limited by its terms to transactions that are electronic. Rather, although all of the transactions described can be performed electronically, all take paper and some take oral forms as well. Indeed, the purpose of the standards, including the security and privacy standards, is stated as ''to enable electronic exchange.'' This purpose would not preclude (and in fact would support) requirements that relate to non-electronic media where they support the overall goal of enabling electronic information exchange. Thus, we believe that the statute authorizes a privacy regulation covering health information in any form or medium maintained or transmitted by the covered entities.

Although we believe that HIPAA authorizes the Secretary to issue regulations covering individually identifiable health information in any form, the proposed privacy standards in this NPRM are directed to protecting only individually identifiable health information that is or at some point has been electronically maintained or transmitted by a covered entity. Those standards do not cover health information that has never been in electronic form.

We are proposing this approach because we believe that it focuses most directly on the primary concern raised by HIPAA: the fact that growing use of computerization in health care, including the rapid growth of electronic transfers of health information, gives rise to a substantial concern about the confidentiality of the health care information that is part of this growing electronic commerce. At the same time, could not adequately address the confidentiality concerns associated with electronic transfers of health information unless we address the resulting uses and disclosures of such information, in whatever form. Indeed, the protection offered by this standard would be devoid of meaning if all non-electronic records and transmissions were excluded. In that event, access to ''protected'' health information would become merely a matter of obtaining the information in a paper or oral form. Such a narrow reading of the statute would lead to a system in which individually identifiable health information transmitted as part of a claim would be protected only until the information was printed or read aloud, at which point protection would disappear. Previously protected information could be freely printed and redistributed, regardless of limits on further electronic redistribution. The statutory language does not compel such an anomalous result.

In developing our proposal, we considered other approaches for determining the information that would be subject to the privacy standards. We considered but rejected limiting the scope of the proposal to information in electronic form. For the reasons discussed above, such a narrow interpretation would render the standards nearly meaningless. We also considered applying the privacy standards to all individually identifiable health information in any form maintained or transmitted by a covered entity. There are clear advantages to this approach, including permitting covered entities to treat all individually identifiable health information under the same standards. We rejected that approach in favor of our proposed approach which we believe is more focused at the public concerns over health information confidentiality in an electronic communications age. We also were concerned about imposing additional burden with respect to health information that was less likely to present privacy concerns: paper records that are never reduced to electronic form are less likely to become disseminated broadly throughout the health care system. We invite comment on the approach that we are proposing and on whether alternate approaches to determining the health information that would be subject to this regulation would be more appropriate.

We also considered making use of other statutory authorities under which we impose general operating or management conditions for programs (e.g., Medicare, grant programs) to enhance these proposed privacy protections. Doing so could enable us to apply these privacy standards to a wider range of entities than are currently affected, such as health care providers who do not transmit standard transactions electronically. We use many other authorities now to impose confidentiality and privacy requirements, although the current rules lack consistency. It is not clear whether using these other authorities would create more uniform protections or expanded enforcement options. Therefore we request comment on the concept of drawing on other authorities to amplify the protections of these privacy standards.

b. *Application to records containing protected and unprotected health information.* Once transmitted or maintained electronically, protected health information is often mixed with unprotected health information in the same record. For example, under the proposed rules, information from a medical record that is electronically transmitted by a provider to a health plan and then returned to the original record would become protected health information, even though the rest of the information contained in the paper record may not be subject to these privacy rules.

We reiterate that under the proposed rule, the protections would apply to the information itself, not to the particular record in which it is contained or transmitted. Therefore, an entity could not maintain duplicate records and only apply the protections to the information contained in the record that is electronically maintained or transmitted. For example, once an individual's name and diagnostic code is transmitted electronically between covered entities (or business partners), that information must be protected by both the transmitting and receiving entities in every record, written, electronic or other, in which it appears.

We recognize that this approach may require some additional administrative attention to mixed records (records containing protected and unprotected health information) to ensure that the handling of protected health information conforms with these regulations. We considered ways to limit application of these protections to avoid such potential administrative concerns. However, these regulations would have little effect if not applicable to otherwise protected health information simply because it was combined with unprotected health information—any information could be lawfully disclosed simply by including some additional information. Likewise, these regulations would have no meaning if entities could then avoid applying the protections merely by maintaining separate duplicate records. A way to limit these rules to avoid application to mixed information without sacrificing basic protections is not apparent.

Unlike the potential issues inherent in the protection of oral information, there may be relatively simple ways to reduce possible confusion in protecting mixed records. The risk of inappropriate use or disclosure of protected health information in a mixed record can be eliminated simply by handling all information in mixed records as if it were protected. It also may be possible to develop a ''watermark'' analogous to a copyright label, designating which written information is protected. We welcome comments on how best to protect information in mixed records, without creating unnecessary administrative burdens.

Finally, we recognize that these rules may create awkward boundaries and enforcement ambiguities, and seek comment on how best to reduce these ambiguities while maintaining the basic protections mandated by the statute.

3. Interaction With Other Standards

The privacy standards in this proposed regulation would be closely integrated with other standards that have been proposed under the HIPAA Administrative Simplification title. This is particularly true with respect to the proposed security standards published on August 12, 1998 (63 FR 43242).

We understand that we are proposing a broader scope of applicability with respect to covered information under these privacy standards than we have previously proposed under the security standard. We intend to solicit additional comments regarding the scope of information that should be addressed under the security standard in the near future.

We also recognize that in this NPRM we are publishing slightly different definitions for some of the concepts that were defined in previously published NPRMs for the other standards. The differences resulted from the comments received on the previous NPRMs as well as the conceptual work done in the development of this NPRM. As we publish the final rules, we will bring all the definitions into conformance.

4. References to Other Laws

The provisions we propose in this rule would interact with numerous other laws. For example, proposed § 164.510 provides standards for certain uses or disclosures that are permitted in this rule, and in some cases references activities that are authorized by other applicable law, such as federal, State, tribal or territorial laws. In cases where this rule references ''law'' or ''applicable law'' we intend to encompass all applicable laws, decisions, rules, regulations, administrative procedures or other actions having the effect of law. We do not intend to exclude any applicable legal requirements imposed by a governmental body authorized to regulate in a given area. Where particular types of law are at issue, such as in the proposed provisions for preemption of State laws in subpart B of part 160, or permitted disclosures related to the Armed Forces in § 164.510(m), we so indicate by referring to the particular type of law in question (e.g., ''State law'' or ''federal law'').

When we describe an action as ''authorized by law,'' we mean that a legal basis exists for the activity. The phrase ''authorized by law'' is a term of art that includes both actions that are permitted and actions that are required by law. When we specifically discuss an action that is ''required'' or ''mandated,'' we mean that a law compels (or conversely, prohibits) the performance of the activity in question. For example, in the health oversight context, disclosure of health information pursuant to a valid Inspector General subpoena, grand jury subpoena, civil investigative demand, or a statute or regulation requiring production of information justifying a claim would constitute a disclosure required by law.

B. Definitions. (§§ 160.103 and 164.504)

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

Section 1171 of the Act defines several terms and our proposed rules would, for the most part, simply restate the law or adopt definitions previously defined in the other HIPAA proposed rules. In some instances, we propose definitions from the Secretary's Recommendations. We also propose some new definitions for convenience and efficiency of exposition, and others to clarify the application and operation of this rule. We describe the proposed definitions and discuss the rationale behind them, below.

Most of the definitions would be defined in proposed §§ 160.103 and 164.504. The definitions at proposed § 160.103 apply to all Administrative Simplification standards, including this privacy rule and the security standard. The definitions proposed in § 164.504 would apply only to this privacy rule. Certain other definitions are specific to particular sections of the proposed rule and are provided in those sections. The terms that are defined at proposed § 160.103 follow:

1. *Act*. We would define ''Act'' to mean the Social Security Act, as amended. This definition would be added for convenience.

2. *Covered entity*. This definition would be provided for convenience of reference and would mean the entities to which part C of title XI of the Act applies. These are the entities described in section 1172(a)(1): Health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction referred to in section 1173(a)(1) of the Act (a ''standard transaction''). In the preamble we occasionally refer to health plans and the health care providers described above as ''covered plans,'' ''covered providers,'' or ''covered plans and providers.''

We note that health care providers who do not submit HIPAA transactions in standard form become covered by this rule when other entities, such as a billing service or a hospital, transmit standard electronic transactions on their behalf. The provider could not circumvent these requirements by assigning the task to its agent, since the agent would be deemed to be acting as the provider.

3. *Health care*. We would define the term ''health care'' as it is defined in the Secretary's Recommendations. Health care means the provision of care, services, or supplies to a patient and includes any: (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure with respect to the physical or mental condition, or functional status, of a patient or affecting the structure or function of the body; (2) sale or dispensing of a drug, device, equipment, or other item pursuant to a prescription; or (3) procurement or banking of blood, sperm, organs, or any other tissue for administration to patients.

4. *Health care clearinghouse*. We would define ''health care clearinghouse'' as defined by section 1171(2) of the Act. The Act defines a ''health care clearinghouse'' as a ''public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.'' In practice, clearinghouses receive transactions from health care providers, health plans, other health care clearinghouses, or business partners of such entities, and other entities, translate the data from a given format into one acceptable to the entity receiving the transaction, and forward the processed transaction to that entity. There are currently a number of private clearinghouses that contract or perform this function for health care providers. For purposes of this rule, we would consider billing services, repricing companies, community health management information systems or community health information systems, ''value-added'' networks, switches and similar organizations to be health care clearinghouses for purposes of this part only if they actually perform the same functions as a health care clearinghouse.

We would note that we are proposing to exempt clearinghouses from a number of the provisions of this rule that would apply to other covered entities (see §§ 164.512, 164.514 and 164.516 below), because in most cases we do not believe that clearinghouses would be dealing directly with individuals. In many instances, clearinghouses would be considered business partners under this rule and would be bound by their contracts with covered plans and providers. See proposed § 164.506(e). We would adopt this position with the caveat that the exemptions would be void for any clearinghouse that had direct contact with individuals in a capacity other than that of a business partner.

5. *Health care provider*. Section 1171(3) of the Act defines ''health care provider'' as a ''provider of medical services as defined in section 1861(u) of the Act, a provider of medical or other health services as defined in section 1861(s) of the Act, and any other person who furnishes health care services or supplies.'' We are proposing to define ''health care provider'' as the Act does, and clarify that a health care provider is limited to any person or organization that furnishes, bills, or is paid for, health care services or supplies in the normal course of business. This definition would include a researcher who provides health care to the subjects of research, free clinics, and a health clinic or licensed health care professional located at a school or business.

Section 1861(u) of the Act contains the Medicare definition of a provider, which encompasses institutional providers, such as hospitals, skilled nursing facilities, home health agencies, and comprehensive outpatient rehabilitation facilities. Section 1861(s) of the Act defines other Medicare facilities and practitioners, including assorted clinics and centers, physicians, clinical laboratories, various licensed/certified health care practitioners, and suppliers of durable medical equipment. The last portion of the proposed definition encompasses appropriately licensed or certified health care practitioners or organizations, including pharmacies and nursing homes and many types of therapists, technicians, and aides. It also would include any other individual or organization that furnishes health care services or supplies in the normal course of business. An individual or organization that bills and/or is paid for health care services or supplies in the normal course of business, such as a group practice or an ''on-line'' pharmacy accessible on the Internet, is also a health care provider for purposes of this statute.

For a more detailed discussion of the definition of health care provider, we refer the reader to our proposed rule (Standard Health Care Provider Identifier) published on May 7, 1998, in the **Federal Register** (63 FR 25320).

6. *Health information*. We would define ''health information'' as it is defined in section 1171(4) of the Act. ''Health information'' would mean any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or

university, or health care clearinghouse; and that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

In this paragraph we attempt to clarify the relationship between the defined terms ''health information,'' ''individually identifiable health information'' and ''protected health information.'' The term ''health information'' encompasses the universe of information governed by the administrative simplification requirements of the Act. For example, under section 1173 of the Act, the Secretary is to adopt standards to enable the electronic exchange of all health information. However, protection of personal privacy is primarily a concern for the subset of health information that is ''individually identifiable health information,'' as defined by the Act (see below). For example, a tabulation of the number of students with asthma by school district would be health information, but since it normally could not be used to identify any individuals, it would not usually create privacy concerns. The definition of individually identifiable health information omits some of the persons or organizations that are described as creating or receiving ''health information.'' Some sections of the Act refer specifically to individually identifiable health information, such as section 1177 in setting criminal penalties for wrongful use or disclosure, and section 264 in requesting recommendations for privacy standards. Finally, we propose the phrase ''protected health information'' (§ 164.504) to refer to the subset of individually identifiable health information that is used or disclosed by the entities that are subject to this rule.

7. *Health plan*. We would define ''health plan'' essentially as section 1171(5) of the Act defines it. Section 1171 of the Act refers to several definitions in section 2791 of the Public Health Service Act, 42 U.S.C. 300gg–91, as added by Public Law 104–191. For clarity, we would incorporate the referenced definitions as currently stated into our proposed definitions.

As defined in section 1171(5), a ''health plan'' is an individual plan or group health plan that provides, or pays the cost of, medical care (see section 2791(a) of the Public Health Service Act (PHS Act)). This definition would include, but is not limited to, the 15 types of plans listed in the statute, as well as any combination of them. The term would include, when applied to public benefit programs, the component of the government agency that administers the program. Church plans and government plans are included to the extent that they fall into one or more of the listed categories.

Health plan'' includes the following singly or in combination:

a. ''Group health plan'' (as currently defined by section 2791(a) of the PHS Act). A group health plan is a plan that has 50 or more participants (as the term ''participant'' is currently defined by section 3(7) of ERISA) or is administered by an entity other than the employer that established and maintains the plan. This definition includes both insured and self-insured plans.

Section 2791(a)(1) of the PHS Act defines ''group health plan'' as an employee welfare benefit plan (as defined in current section 3(1) of ERISA) to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, or otherwise.

b. ''Health insurance issuer'' (as currently defined by section 2791(b) of the PHS Act).

Section 2971(b) of the PHS Act defines a ''health insurance issuer'' as an insurance company, insurance service, or insurance organization that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance.

c. ''Health maintenance organization'' (as currently defined by section 2791(b) of the PHS Act). Section 2791(b) of the PHS Act currently defines a ''health maintenance organization'' as a federally qualified health maintenance organization, an organization recognized as such under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such a health maintenance organization. These organizations may include preferred provider organizations, provider sponsored organizations, independent practice associations, competitive medical plans, exclusive provider organizations, and foundations for medical care.

d. Part A or Part B of the Medicare program (title XVIII of the Act).

e. The Medicaid program (title XIX of the Act).

f. A ''Medicare supplemental policy'' as defined under section 1882(g)(1) of the Act. Section 1882(g)(1) of the Act defines a ''Medicare supplemental policy'' as a health insurance policy that a private entity offers a Medicare beneficiary to provide payment for expenses incurred for services and items that are not reimbursed by Medicare because of deductible, coinsurance, or other limitations under Medicare. The statutory definition of a Medicare supplemental policy excludes a number of plans that are similar to Medicare supplemental plans, such as health plans for employees and former employers and for members and former members of trade associations and unions. A number of these health plans may be included under the definitions of ''group health plan'' or ''health insurance issuer,'' as defined in paragraphs ''a'' and ''b'' above.

g. A ''long-term care policy,'' including a nursing-home fixed indemnity policy. A ''long-term care policy'' is considered to be a health plan regardless of how comprehensive it is.

h. An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers. This includes plans that are referred to as multiple employer welfare arrangements (''MEWAs'').

i. The health care program for active military personnel under title 10 of the United States Code. See paragraph ''k'', below, for further discussion.

j. The veterans health care program under chapter 17 of title 38 of the United States Code. This health plan primarily furnishes medical care through hospitals and clinics administered by the Department of Veterans Affairs (VA) for veterans enrolled in the VA health care system.

k. The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) as defined in 10 U.S.C. 1072(4). We note that the Act's definition of ''health plan'' omits several types of health care provided by the Department of Defense (DOD). Sections 1171(5)(I) and 1171(5)(K) cover only the health care program for active duty personnel (see 10 U.S.C. 1074(a)) and the CHAMPUS program (see 10 U.S.C. 1079, 1086). What is omitted is health care provided in military treatment facilities to military retirees (see 10 U.S.C. 1074(b)), to dependents of active duty personnel and to dependents of retirees (see 10 U.S.C. 1076), to Secretarial designees such as members of Congress, Justices of the Supreme Court, and to foreign military personnel under NATO status of forces agreements. Health care provided by the DOD in military facilities to the aforementioned persons is not included as a ''health plan'' under HIPAA. However, these facilities would still be considered to be health care providers.

l. The Indian Health Service program under the Indian Health Care Improvement Act (25 U.S.C. 1601, *et.*

seq.). This program furnishes services, generally through its own health care providers, primarily to persons who are eligible to receive services because they are of American Indian or Alaskan Native descent.

m. The Federal Employees Health Benefits Program under 5 U.S.C. chapter 89. This program consists of health insurance plans offered to active and retired federal employees and their dependents. Although section 1171(5)(M) of the Act refers to the ''Federal Employees Health Benefit Plan,'' this and any other rules adopting administrative simplification standards will use the correct name, the Federal Employees Health Benefits Program. One health plan does not cover all federal employees; over 350 health plans provide health benefits coverage to federal employees, retirees, and their eligible family members. Therefore, we will use the correct name, The Federal Employees Health Benefits Program, to make clear that the administrative simplification standards apply to all health plans that participate in the Program.

n. An approved State child health plan for child health assistance that meets the requirements of section 2103 of the Act, which established the Children's Health Insurance Program (CHIP).

o. A Medicare Plus Choice organization as defined in 42 CFR 422.2, with a contract under 42 CFR part 422, subpart K.

p. Any other individual plan or group health plan, or combination thereof, that provides or pays for the cost of medical care. This category implements the language at the beginning of the statutory definition of the term ''health plan'': ''The term 'health plan' means an individual or group plan that provides, or pays the cost of, medical care * * * Such term includes the following, and any combination thereof * * *'' This statutory language is general, not specific. Moreover, the statement that the term ''health plan'' ''includes'' the specified plans implies that the term also covers other plans that meet the stated criteria. One approach to interpreting this introductory language in the statute would be to make coverage decisions about plans that may meet these criteria on a case-by-case basis. Instead we propose to clarify its coverage by adding this category to the proposed definition of ''health plan''; we seek public comment on its application. The Secretary would determine which plans that meet the criteria in the preceding paragraph are health plans for purposes of title II of HIPAA.

Consistent with the other parts of HIPAA, the provisions of this rule generally would not apply to certain types of insurance entities, such as workers' compensation and automobile insurance carriers, other property and casualty insurers, and certain forms of limited benefits coverage, even when such arrangements provide coverage for health care services. 29 U.S.C. 1186(c). We note that health care providers would be subject to the provisions of this rule with respect to the health care they provide to individuals, even if such providers seek or receive reimbursement from an insurance entity that is not a covered entity under these rules. However, nothing in this rule would be intended to prevent a health care provider from disclosing protected health information to a non-covered insurance entity for the purpose of obtaining payment for services. Further, under proposed § 164.510(n), this rule would permit disclosures by health care providers of protected health information to such insurance entities and to other persons when mandated by applicable law for the purposes of determining eligibility for coverage or benefits under such insurance arrangements. For example, a State workers' compensation law that requires disclosure of protected health information to an insurer or employer for the purposes of determining an individual's eligibility for medical or other benefits, or for the purpose of determining fitness for duty, would not be disturbed by this rule.

8. *Secretary.* This term means the Secretary of Health and Human Services and any other officer or employee of the Department of Health and Human Services to whom the authority involved has been delegated. It is provided for ease of reference.

9. *Small health plan.* The HIPAA does not define a ''small health plan,'' but instead explicitly leaves the definition to be determined by the Secretary. We propose to adopt the size classification used by the Small Business Administration. We would therefore define a ''small health plan'' as a health plan with annual receipts of $5 million or less. 31 CFR 121.201. This differs from the definition of ''small health plan'' in prior proposed Administrative Simplification rules. We will conform the definitions in the final Administrative Simplification rules.

10. *Standard.* The term ''standard'' would mean a prescribed set of rules, conditions, or requirements concerning classification of components, specification of materials, performance or operations, or delineation of procedures in describing products, systems, services, or practices. This definition is a general one, to accommodate the varying functions of the specific standards proposed in the other HIPAA regulations, as well as the rules proposed below.

11. *State.* This term would include the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam. This definition follows the statutory definition of ''State'' in section 1101(a) of the Act.

12. *Transaction.* We would define ''transaction,'' as we have done in other Administrative Simplification regulations, to mean the exchange of information between two parties to carry out financial or administrative activities related to health care. A transaction would be (1) any of the transactions listed in section 1173(a)(2) of the Act, and (2) any transaction determined appropriate by the Secretary in accordance with Section 1173(a)(1) of the Act.

A ''transaction'' would mean any of the following:

a. *Health claims or equivalent encounter information.* This transaction could be used to submit health care claim billing information, encounter information, or both, from health care providers to payers, either directly or via intermediary billers and claims clearinghouses.

b. *Health care payment and remittance advice.* This transaction could be used by a health plan to make a payment to a financial institution for a health care provider (sending payment only), to send an explanation of benefits remittance advice directly to a health care provider (sending data only), or to make payment and send an explanation of benefits remittance advice to a health car provider via a financial institution (sending both payment and data).

c. *Coordination of benefits.* This transaction could be used to transmit health care claims and billing payment information between payers with different payment responsibilities where coordination of benefits is required or between payers and regulatory agencies to monitor the furnishing, billing, and/ or payment of health care services within a specific health care/insurance industry segment.

d. *Health claims status.* This transaction could be used by health care providers and recipients of health care products or services (or their authorized agents) to request the status of a health care claim or encounter from a health plan.

e. *Enrollment and disenrollment in a health plan.* This transaction could be used to establish communication between the sponsor of a health benefit and the payer. It provides enrollment data, such as subscriber and dependents, employer information, and primary care health care provider information. A sponsor would be the backer of the coverage, benefit, or product. A sponsor could be an employer, union, government agency, association, or insurance company. The health plan would refer to an entity that pays claims, administers the insurance product or benefit, or both.

f. *Eligibility for a health plan.* This transaction could be used to inquire about the eligibility, coverage, or benefits associated with a benefit plan, employer, plan sponsor, subscriber, or a dependent under the subscriber's policy. It also could be used to communicate information about or changes to eligibility, coverage, or benefits from information sources (such as insurers, sponsors, and payers) to information receivers (such as physicians, hospitals, third party administrators, and government agencies).

g. *Health plan premium payments.* This transaction could be used by, for example, employers, employees, unions, and associations to make and keep track of payments of health plan premiums to their health insurers. This transaction could also be used by a health care provider, acting as liaison for the beneficiary, to make payment to a health insurer for coinsurance, copayments, and deductibles.

h. *Referral certification and authorization.* This transaction could be used to transmit health care service referral information between health care providers, health care providers furnishing services, and payers. It could also be used to obtain authorization for certain health care services from a health plan.

i. *First report of injury.* This transaction could be used to report information pertaining to an injury, illness, or incident to entities interested in the information for statistical, legal, claims, and risk management processing requirements.

j. *Health claims attachments.* This transaction could be used to transmit health care service information, such as subscriber, patient, demographic, diagnosis, or treatment data for the purpose of a request for review, certification, notification, or reporting the outcome of a health care services review.

k. *Other transactions as the Secretary may prescribe by regulation.* Under section 1173(a)(1)(B) of the Act, the Secretary may adopt standards, and data elements for those standards, for other financial and administrative transactions deemed appropriate by the Secretary. These transactions would be consistent with the goals of improving the operation of the health care system and reducing administrative costs.

In addition to the above terms, a number of terms are defined in proposed § 164.504, and are specific to the proposed privacy rules. They are as follows:

13. *Business partner.* This term would mean a person to whom a covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. Such term includes any agent, contractor or other person who receives protected health information from the covered entity (or from another business partner of the covered entity) for the purposes described in the previous sentence. It would not include a person who is an employee, a volunteer or other person associated with the covered entity on a paid or unpaid basis.

14. *Designated record set.* This term would be defined as a group of records under the control of a 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, and which is used by the covered entity to make decisions about the individual. The concept of a ''designated record set'' is derived from the Privacy Act's concept of a ''system of records.'' 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, we would substitute the term ''covered entity'' for ''agency'' and limit the information to that used by the covered entity to make decisions about the individual.

We would define a ''record'' as ''any item, collection, or grouping of protected health information maintained, collected, used, or disseminated by a covered entity.'' Under the Privacy Act, ''the term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.'' 5 U.S.C. 552a(a)(4). For purposes of this rule we propose to limit the information to protected health information, as defined in this rule. ''Protected health information'' already incorporates the concept of identifiability, and therefore our definition of ''record'' is much simpler.

For health plans, designated record sets would include, at a minimum, the claims adjudication, enrollment, and patient accounting systems. For health care providers, designated record sets would include, at a minimum, the medical records and billing records. Designated record set would also include a correspondence system, a complaint system, or an event tracking system if decisions about individuals are made based, in whole or in part, on information in those systems. 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 would not fall under this definition.

We note that a designated record set would only exist for types of records that a covered entity actually ''retrieves'' 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.

15. *Disclosure.* This term would be defined as the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

16. *Health care operations.* We propose the term ''health care operations'' to clarify the activities we consider to be ''compatible with and directly related to'' treatment and payment and therefore would not require authorization from the individual for use or disclosure of protected health information.

Under our proposal, ''health care operations'' means the following services or activities if provided by or on behalf of a covered health plan or health care provider for the purposes of carrying out the management functions of such plan or provider necessary for the support of treatment or payment:

- Conducting quality assessment and improvement activities, including evaluating outcomes, and developing clinical guidelines;

• Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which undergraduate and graduate students and trainees in all areas of health care learn under supervision to practice as health care providers (e.g., residency programs, grand rounds, nursing practicums), accreditation, certification, licensing or credentialing activities;

• Insurance rating and other insurance activities relating to the renewal of a contract for insurance, including underwriting, experience rating, and reinsurance, but only when the individuals are already enrolled in the health plan conducting such activities and only when the use or disclosure of such protected health information relates to an existing contract of insurance (including the renewal of such a contract);

• Conducting or arranging for auditing services, including fraud and abuse detection and compliance programs; and

• Compiling and analyzing information in anticipation of, or for use in, civil or criminal legal proceedings.

Our definition proposes to limit health care operations to functions and activities performed by a health plan or provider or by a business partner on behalf of a health plan or a provider. Our definition anticipates that in order for treatment and payment to occur, protected health information would be used within entities, would be shared with business partners, and in some cases would be shared between covered entities (or their business partners). However, a health care operation should not result in protected health information being disclosed to an entity that is not the covered entity (or a business partner of such entity) on whose behalf the operation is being performed. For example, a health plan may request a health care provider to provide protected health information to the health plan, or to a business partner of the health plan, as part of an outcomes evaluation effort relating to providers affiliated with that plan. This would be a health care operation.

We are aware that the health care industry is changing and that these categories, though broad, may need to be modified to reflect different conditions in the future.

17. *Health oversight agency.* We would define the term ''health oversight agency'' as it is defined in the Secretary's Recommendations. See section II.E. below for further discussion.

18. *Individual.* We would define ''individual'' to mean the person who is the subject of protected health information. We would define the term to include, with respect to the signing of authorizations and other rights (such as access, copying, and correction), various types of legal representatives. The term would include court-appointed guardians or persons with a power of attorney, including persons making health care decisions for incapacitated persons, persons acting on behalf of a decedent's estate, where State or other applicable law authorizes such legal representatives to exercise the person's rights in such contexts, and parents subject to certain restrictions explained below. We would define this term to exclude foreign military and foreign diplomatic personnel and their dependents who receive health care provided or paid for by the DOD or other federal agency or entity acting on its behalf, and overseas foreign national beneficiaries of health care provided by the DOD or other federal agency, or non-governmental organization acting on its behalf.

a. *Disclosures pursuant to a power of attorney.* The definition of an individual would include legal representatives, to the extent permitted under State or other applicable law. We considered several issues in making this determination.

A ''power of attorney'' is a legal agreement through which a person formally grants authority to another person to make decisions on the person's behalf about financial, health care, legal, and/or other matters. In granting power of attorney, a person does not give up his or her own right to make decisions regarding the health care, financial, legal, or other issues involved in the legal agreement. Rather, he or she authorizes the other person to make these decisions as well.

In some cases, an individual gives another person power of attorney over issues not directly related to health care (e.g., financial matters) while informally relying on a third person (either implicitly or through verbal agreement) to make health care decisions on his or her behalf. In such situations, the person with power of attorney could seek health information from a health plan or provider in order to complete a task related to his or her power of attorney. For example, a person with financial power of attorney may request health information from a health plan or provider in order to apply for disability benefits on the individual's behalf.

In developing proposed rules to address these situations, we considered two options: (1) Allowing health plans and health care providers to disclose health information without authorization directly to the person with power of attorney over issues not directly related to health care; and (2) prohibiting health plans or health care providers from disclosing health information without authorization directly to such persons and stating that disclosure without authorization is permitted only to persons designated formally (through power of attorney for health care) or informally as the patient's health care decision-maker. We believe that both options have merit.

The first option recognizes that the responsibilities of persons with power of attorney often are broad, and that even when the power of attorney agreement does not relate directly to health care, the person with power of attorney at times has a legitimate need for health information in order to carry out his or her legal responsibility. The second option recognizes that when an individual is competent to make health care decisions, it is appropriate for him or her (or, if the individual wishes, for the informally designated health care decision maker) to decide whether the covered entity should disclose health information to someone with power of attorney over issues not directly related to health care.

In light of the fact that laws vary by State regarding power of attorney and that implementation of either option could be in the individual's interest, we would allow health plans and health care providers to disclose protected health information without authorization directly to persons with power of attorney to handle any issue on the individual's behalf, in accordance with State or other applicable laws regarding this issue.

This definition also accounts for situations in which a competent individual has granted one person power of attorney over health care issues yet, in practice, relies on another person to make health care decisions. We recognize that, by giving power of attorney for health care issues to one person and involving another person informally in making treatment decisions, the individual is, in the first instance, formally granting consent to release his or her health information and, in practice, granting consent to release medical information to the second person. Therefore, we would allow a health plan or provider, pursuant to State or other applicable law, to disclose protected health information without authorization to a person with power of attorney for the patient's health care and to a person informally designated as the patient's health care decision maker.

b. *Disclosures pertaining to incapacitated individuals.* Covered entities would be permitted to disclose protected health information to any person making health care decisions for an incapacitated person under State or other applicable law. This definition defers to current laws regarding health care decision-making when a patient is not a minor and is incapable of making his or her own decisions. We propose to permit information to follow such decision-making authority. It is our intent not to disturb existing practices regarding incapacitated patients.

Applicable laws vary significantly regarding the categories of persons who can make health care decisions when a patient is incapable of making them. For example, some State laws establish a hierarchy of persons who may make medical decisions for the incapacitated person (e.g., first a person with power of attorney, if not then next-of-kin, if none then close friend, etc.). In other States, health care providers may exercise professional judgment about which person would make health care decisions in the patient's best interest. We also recognize that federal agencies have, in some cases, established rules regarding such patients. For example, the DOD has established requirements regarding military personnel who are based overseas and who have become incapable of making their own decisions.

Because laws vary regarding patients unable to make their own decisions and because these patients' interests could be served through a variety of arrangements, we would allow health plans and health care providers to disclose information in accordance with applicable laws regarding incapacitated patients.

c. *Disclosures pertaining to minors.* In general, because the definition of individual would include parents, a parent, guardian, or person acting *in loco parentis* could exercise the rights established under this regulation on behalf of their minor (as established by applicable law) children. However, in cases where a minor lawfully obtains a health care service without the consent of or notification to a parent, the minor would be treated as the individual for purposes of exercising any rights established under this regulation with respect to protected health information relating to such health services. Laws regarding access to health care for minors and confidentiality of their medical records vary widely; this proposed regulation recognizes and respects the current diversity of the law in this area. It would not affect applicable regulation of the delivery of health care services to minors, and would not preempt any law authorizing or prohibiting disclosure of individually identifiable health information of minor individuals to their parents. The disclosure of individually identifiable health information from substance abuse records is also addressed by additional requirements established under 42 CFR part 2.

d. *Foreign recipients of defense related health care.* We would define the term ''individual'' to exclude foreign military and foreign 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. We would also exclude from this term overseas foreign national beneficiaries of health care provided by the DOD or other federal agency or by a non-governmental organization acting on behalf of DOD or such agency. This exclusion is discussed in section II.E.l3.

e. *Disclosures pertaining to deceased persons.* This provision is discussed in Section II.C.6.

19. *Individually identifiable health information.* We would define ''individually identifiable health information'' as it is defined in section 1171(6) of the Act. While the definition of individually identifiable health information does not expand on the statutory definition, we recognize that the issue of how the identifying characteristics can be removed from such information (referred to in this rule as de-identification) presents difficult operational issues. Accordingly, we propose in § 164.506(d) an approach for de-identifying identifiable information, along with restrictions designed to ensure that de-identified information is not used inappropriately.

The privacy standards would apply to ''individually identifiable health information,'' and not to information that does not identify the individual. We are aware that, even after removing obvious identifiers, there is always some probability or risk, however remote, that any information about an individual can be attributed. A 1997 MIT study showed that, because of the public availability of the Cambridge, Massachusetts voting list, 97 percent of the individuals in Cambridge whose data appeared in a data base which contained only their nine digit zip code and birth date could be identified with certainty.[1] Their information had been ''de-identified'' (some obvious identifiers had been removed) but it was not anonymous (it was still possible to identify the individual).

It is not always obvious when information identifies the subject. If the name and identifying numbers (e.g., SSN, insurance number, etc.) are removed, a person could still be identified by the address. With the address removed, the subject of a medical record could be identified based on health and demographic characteristics (e.g., age, race, diagnosis). ''Identifiability'' varies with the location of the subject; there could be hundreds of people in Manhattan who have the same age, race, gender, and diagnosis, but only one such person in a small town or rural county. Gauging the risk of identification of information requires statistical experience and expertise that most covered entities will not possess.

Obvious identifiers on health information could be replaced with random numbers or encrypted codes, which can prevent the person using the record from identifying the subject, but which allow the person holding the code to re-identify the information. Information with coded or encrypted identifiers would be considered ''de-identified'' but not ''anonymous,'' because it is still possible for someone to identify the subject.

We considered defining ''individually identifiable health information'' as any information that is not anonymous, that is, for which there is any possibility of identifying the subject. We rejected this option, for several reasons. First, the statute suggests a different approach. The term ''individually identifiable health information'' is defined in HIPAA as health information that ''* * * identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.'' By including the modifier ''reasonable basis,'' Congress appears to reject the absolute approach to defining ''identifiable.''

Second, covered entities may not have the statistical sophistication to know with certainty when sufficient identifying information has been removed so that the record is no longer identifiable. We believe that covered entities need more concrete guidance as to when information will and will not be ''identifiable'' for purposes of this regulation.

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

Finally, defining non-identifiable to mean anonymous would require covered entities to comply with the terms of this regulation with respect to information for which the probability of identification of the subject is very low. We want to encourage covered entities and others to remove obvious identifiers or encrypt them whenever possible; use of the absolute definition of ''identifiable'' would not promote this salutary result.

For these reasons, we propose at § 164.506(d)(2)(ii) that there be a presumption that, if specified identifying information is removed and if the holder has no reason to believe that the remaining information can be used by the reasonably anticipated recipients alone or in combination with other information to identify an individual, then the covered entity is presumed to have created de-identified information.

At the same time, in proposed § 164.506(d)(2)(iii), we would leave leeway for more sophisticated data users to take a different approach. We would include a ''reasonableness'' standard so that entities with sufficient statistical experience and expertise could remove or code a different combination of information, so long as the result is still a low probability of identification. With this approach, our intent is to provide certainty for most covered entities, while not limiting the options of more sophisticated data users.

In § 164.504, we propose to define ''individually identifiable health information'' to mean health information created or received by a health care provider, health plan, employer or health care clearinghouse, that could be used directly or indirectly to identify the individual who is the subject of the information. Under proposed § 164.506(d)(2)(ii), information would be presumed not to be ''identifiable'' if:

- All of the following data elements have been removed or otherwise concealed: Name; address, including street address, city, county, zip code, or equivalent geocodes; names of relatives and employers; birth date; telephone and fax numbers; e-mail addresses; social security number; medical record number; health plan beneficiary number; account number; certificate/license number; any vehicle or other device serial number; web URL; Internet Protocol (IP) address; finger or voice prints; photographic images; and any other unique identifying number, characteristic, or code (whether generally available in the public realm or not) that the covered entity has reason to believe may be available to an anticipated recipient of the information, and
- The covered entity has no reason to believe that any reasonably anticipated recipient of such information could use the information alone, or in combination with other information, to identify an individual. Thus, to create de-identified information, entities that had removed the listed identifiers would still have to remove additional data elements if they had reason to believe that a recipient could use the remaining information, alone or in combination with other information, to identify an individual. For example, if the ''occupation'' field is left intact and the entity knows that a person's occupation is sufficiently unique to allow identification, that field would have to be removed from the relevant record. The presumption does not allow use or disclosure if the covered entity has reason to believe the subject of the information can be re-identified. Our concern with the potential for re-identification is heightened by our limited jurisdiction under HIPAA. Because we can only regulate health care providers, health plans and health care clearinghouses, we cannot prohibit other recipients of de-identified information from attempting to re-identify it.

To assist covered entities in ascertaining whether their attempts to create de-identified information would be successful, the Secretary would from time to time issue guidance establishing methods that covered entities could use to determine the identifiability of information. This guidance would include information on statistical and other tests that could be performed by covered entities in assessing whether they have created de-identified information. The manner in which such guidance would be published and distributed will be addressed in the final regulation. We solicit comment on the best ways in which to inform covered entities of appropriate and useful information on methods that they can use to determine whether information is de-identified.

In enforcing this regulation, the Secretary would consider the sophistication of covered entities when determining whether a covered entity had reason to believe that information that it had attempted to de-identify continued to identify the subject. Covered entities that routinely create and distribute de-identified data would be expected to be aware of and to use advanced statistical techniques, including the guidance issued by the Secretary, to ensure that they are not improperly disclosing individually identifiable health information. Covered entities that rarely create de-identified information would not be expected to have the same level of knowledge of these statistical methods, and generally could rely on the presumption that information from which they have removed the listed identifiers (and provided that they do not know that the information remains identifiable) is de-identified. We solicit comment on whether the enforcement approach that we are suggesting here and our overall approach relating to the creation of de-identified information would provide sufficient guidance to covered entities to permit them to create, use and disclose de-identified information.

In addition, we propose to permit entities with appropriate statistical experience and expertise (obtained through a statistical consultant or staff with statistical expertise) to decide that some of the above named data elements could be retained in the de-identified data set if: (1) The entity determines that the probability of identifying an individual with the remaining information is very low, or (2) the entity has converted the ''identifiable'' data elements into data elements that, in combination with the remaining information, have a very low probability of being used to identify an individual. An example of such a conversion would be the translation of birth date into age expressed in years or, if still determined to convey ''identifiability,'' age expressed in categories of years (e.g., age 18 to 24). In making these determinations, the entity must consider the data elements taken together as well as any additional information that might reasonably be available to a recipient. Examples of the types of entities that would have the statistical experience and expertise to make this type of judgment include large health research institutions such as medical schools with epidemiologists and statisticians on the faculty; federal agencies such as the National Center for Health Statistics, the Agency for Health Care Policy and Research, FDA, the Bureau of the Census, and NIH; and large corporations that do health research such as pharmaceutical manufacturers with epidemiologists and statisticians on staff.

An important component of this approach to defining ''identifiable'' would be the prohibition on re-identification of health information. We propose that a covered entity that is a recipient of de-identified information who attempts to re-identify such de-identified information for a purpose for which protected health information could not be used or disclosed under this rule be deemed to be in violation of the law. See proposed § 164.506(d) and section II.C. below. There may be circumstances, however, when recipients of de-identified information will have a legitimate reason to request that the de-identified information be re-identified by the originating covered entity. For example, if a researcher received de-identified information from a covered entity and the research revealed that a particular patient was misdiagnosed, the covered entity should be permitted to re-identify the patient's health information so that the patient could be informed of the error and seek appropriate care. One of the principal reasons entities retain information in coded form, rather than rendering it anonymous, is to enable re-identification of the information for appropriate reasons. Although we would anticipate that the need for re-identification would be rare, entities that expect to have to perform this function should establish a process for determining when re-identification is appropriate. Once covered entities re-identify information, it becomes protected information and may, therefore, be used and disclosed only as permitted by this regulation.

The phrase ''individually identifiable'' information is already in use by many HHS agencies and others. In particular, the Common Rule regulation includes ''identifiable private information'' in its definition of ''human subject.'' Because of this, medical records research on ''identifiable private information'' is subject to Common Rule consent and IRB review requirements. It would not be our intent to suggest changes to this practice. Researchers and others can and are encouraged to continue to use more stringent approaches to protecting information.

We invite comment on the approach that we are proposing and on alternative approaches to standards for covered entities to determine when health information can reasonably be considered no longer individually identifiable.

20. *Law enforcement official.* We propose a new definition of ''law enforcement official,'' to mean an officer of the United States or a political subdivision thereof, who is empowered by law to conduct an investigation or official proceeding inquiring into a violation of, or failure to comply with, any law; or a criminal, civil, or administrative proceeding arising from a violation of, or failure to comply with, any law.

21. *Payment.* We offer a new definition of payment. The term ''payment'' would mean activities undertaken by a health plan (or by a business partner on behalf of a health plan) to determine its responsibilities for coverage under the health plan policy or contract including the actual payment under the policy or contract, or by a health care provider (or by a business partner on behalf of a provider) to obtain reimbursement for the provision of health care, including:

- Determinations of coverage, improving payment methodologies or coverage policies, or adjudication or subrogation of claims;
- Risk adjusting payments based on enrollee health status and demographic characteristics;
- Billing, claims management, medical review, medical data processing;
- Review of health care services with respect to medical necessity, coverage under a health plan policy or contract, appropriateness of care, or justification of charges; and,
- Utilization review activities, including pre-certification and preauthorization of services.

Our proposed definition is intended to capture the necessary sharing of protected health information among health care providers who provide care, health plans and other insurers who pay for care, their business partners, as well as sponsors of group health plans, such as employers, who pay for care and sometimes provide administrative services in conjunction with health plan payment activities. For example, employers sometimes maintain the eligibility file with respect to a group health plan.

Our proposed definition anticipates that protected health information would be used for payment purposes within entities, would be shared with business partners, and in most cases would be shared between health care providers and health plans (and their business partners). In some cases, a payment activity could result in the disclosure of protected health information by a plan to an employer or to another payer of health care, or to an insurer that is not a covered entity, such as for coordination of benefits or to a workers compensation carrier. For example, a health plan could disclose protected health information to an employer in connection with determining the experience rate for group coverage.

We are concerned that disclosures for payments may routinely result in disclosures of protected health information to non-covered entities, such as employers, which are not subject to the use and disclosure requirements of this rule. We considered prohibiting disclosures to employers without individual authorization, or alternatively, requiring a contractual relationship, similar to the contracts required for business partners, before such disclosures could occur. We note that the National Committee on Quality Assurance has adopted a standard for the year 2000 that would require health plans to ''have policies that prohibit sending identifiable personal health information to fully insured or self-insured employers and provide safeguards against the use of information in any action relating to an individual'' (Standard R.R.6, National Committee for Quality Assurance 2000 Standards).

We did not adopt either of these approaches, however, because we were concerned that we might disrupt some beneficial activities if we were to prohibit or place significant conditions on disclosures by health plans to employers. We also recognize that employers are paying for health care in many cases, and it has been suggested to us that they may need access to claims and other information for the purposes of negotiating rates, quality improvement and auditing their plans and claims administrators. We invite comment on the extent to which employers currently receive protected health information about their employees, for what types of activities protected health information is received, and whether any or all of these activities could be accomplished with de-identified health information. We also invite other comments on how disclosures to employers should be treated under this rule.

22. *Protected health information.* We would create a new definition of ''protected health information'' to mean individually identifiable health information that is or has been electronically maintained or electronically transmitted by a covered entity, as well as such information when it takes any other form. For example, protected health information would remain protected after it is read from a computer screen and discussed orally, printed onto paper or other media, photographed, or otherwise duplicated. We note that individually identifiable health information created or received by an employer as such would not be considered protected health information, although such information created or received by an employer in its role as a health plan or provider would be protected health information.

Under this definition, information that is ''electronically transmitted'' would include information exchanged with a computer using electronic media, even when the information is physically moved from one location to another using magnetic or optical media (e.g., copying information from one computer to another using a floppy disc). Transmissions over the Internet (i.e., open network), Extranet (i.e., using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks would all be included. Telephone voice response and ''faxback'' (i.e., a request for information from a computer made via voice or telephone keypad input with the requested information returned as a fax) systems would be included because these are computer output devices similar in function to a printer or video screen. This definition would not include ''paper-to-paper'' faxes, or person-to-person telephone calls, video teleconferencing, or messages left on voice-mail. The key concept that determines if a transmission meets the definition is whether the source or target of the transmission is a computer. The medium or the machine through which the information is transmitted or rendered is irrelevant.

Also, information that is ''electronically maintained'' would be information stored by a computer or on any electronic medium from which the information may be retrieved by a computer. These media include, but are not limited to, electronic memory chips, magnetic tape, magnetic disk, or compact disc (CD) optical media.

Individually identifiable health information that is part of an ''education record'' governed by the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, would not be considered protected health information. Congress specifically addressed such information when it enacted FERPA to protect the privacy rights of students and parents in educational settings. FERPA applies to educational records that are maintained by educational agencies and institutions that are recipients of federal funds from the Department of Education. FERPA requires written consent of the parent or student prior to disclosure of education records except in statutorily specified circumstances. We do not believe that Congress intended to amend or preempt FERPA in enacting HIPAA.

Individually identifiable health information of inmates of correctional facilities and detainees in detention facilities would be excluded from this definition because unimpeded sharing of inmate identifiable health information is crucial for correctional and detention facility operations. In a correctional or detention setting, prison officials are required by law to safely house and provide health care to inmates. These activities require the use and disclosure of identifiable health information. Therefore, correctional and detention facilities must routinely share inmate health information among their health care and other components, as well as with community health care facilities. In order to maintain good order and protect the well-being of prisoners, the relationship between such facilities and inmates or detainees involves a highly regulated, specialized area of the law which has evolved as a carefully balanced compromise with due deference to institutional needs and obligations.

Federal and other prison facilities routinely share health information with community health care facilities in order to provide medical treatment to persons in their custody. It is not uncommon for inmates and detainees to be transported from one facility to another, for example, for the purpose of making a court appearance in another jurisdiction, or to obtain specialized medical care. In these and other circumstances, law enforcement agencies such as the Federal Bureau of Prisons (the Bureau), the United States Marshals Service (USMS), the Immigration and Naturalization Service, State prisons, county jails, and U.S. Probation Offices, share identifiable health information about inmates and detainees to ensure that appropriate health care and supervision of the inmate or detainee is maintained. Likewise, these agencies must, in turn, share health information with the facility that resumes custody of the inmate or detainee.

Requiring an inmate's or detainee's authorization for disclosure of identifiable health information for day-to-day operations would represent a significant shift in correctional and detention management philosophy. If correctional and detention facilities were covered by this rule, the proposed provisions for individual authorizations could potentially be used by an inmate or detainee to override the safety and security concerns of the correctional/custodial authority; for example, an inmate being sent out on a federal writ could refuse to permit the Bureau to disclose a suicide history to the USMS. Additionally, by seeking an authorization to disclose the information, staff may give the inmate or detainee advance notice of an impending transfer, which in turn may create security risks.

Therefore we propose to exclude the individually identifiable health information of inmates of correctional facilities and detainees in detention facilities from the definition of protected health information. We note that existing federal laws limiting the disclosure and release of information (e.g., FOIA/Privacy Act) protect the privacy of identifiable federal inmate health information. Subject to certain limitations, these laws permit inmates and detainees to obtain and review a copy of their medical records and to correct inaccurate information.

Under this approach, the identifiable health information held by correctional and detention facilities of persons who have been released would not be protected. The facilities require continued access to such information for security, protection and health care purposes because inmates and detainees are frequently readmitted to correctional and detention facilities. However, concern has been expressed about the possibility that absent coverage by this proposed rule, correctional and detention facilities may disclose information about former inmates and detainees without restriction. We therefore request comments on whether identifiable health information held by correctional and detention facilities about former inmates and detainees should be subject to this rule, and the potential security concerns and burden such a requirement might place on these facilities.

23. *Psychotherapy notes.* We would define ''psychotherapy notes'' to mean detailed notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session. Such notes are used only by the therapist who wrote them, maintained separately from the medical record, and not involved in the documentation necessary for health care treatment, payment, or operations. Such term would not include medication prescription and monitoring, counseling session start and stop times or the modalities and frequencies of treatment furnished, results of clinical tests, or a brief summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis and progress to date.

24. *Public health authority.* We would define ''public health authority'' as an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe that is responsible for public health matters as part of its official mandate.

25. *Research.* We would define ''research'' as a systematic investigation,

including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. We further explain that ''generalizable knowledge'' is knowledge related to health that can be applied to populations outside of the population served by the covered entity.

This is the definition of ''research'' in the federal regulation that protects human subjects, entitled The Federal Policy for the Protection of Human Subjects (often referred to as the ''Common Rule,'' at 45 CFR part 46). 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.

26. *Research information unrelated to treatment.* We would define ''research information unrelated to treatment'' as information that is received or created by a covered entity in the course of conducting research for which there is insufficient scientific and medical evidence regarding the validity or utility of the information such that it should not be used for the purpose of providing health care,[2] and with respect to which the covered entity has not requested payment from a health plan.

27. *Treatment.* We would define ''treatment'' to mean the provision of health care by, or the coordination of health care (including health care management of the individual through risk assessment, case management, and disease management) among, health care providers, or the referral of an individual from one provider to another, or coordination of health care or other services among health care providers and third parties authorized by the health plan or the individual. Our definition is intended to relate only to services provided to an individual and not to an entire enrolled population.

28. *Use.* We would propose a new definition of the term ''use'' to mean the employment, application, utilization, examination or analysis of health information within an entity that holds the information.

29. *Workforce.* We would define ''workforce'' to mean employees, volunteers, trainees and other persons under the direct control of a covered entity, including persons providing labor on an unpaid basis.

[2] For example, *validity* is an indicator of how well a test measures the property or characteristic it is intended to measure and the reliability of a test, *i.e.*, whether the same result is obtained each time the test is used. Validity is also a measurement of the accuracy with which a test predicts a clinical condition. *Utility* refers to the degree to which the results of test can be used to make decisions about the subsequent delivery of health care.

C. General Rules. (§ 164.506)

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

The purpose of our proposal is to define and limit the circumstances in which an individual's protected health information could be used or disclosed by covered entities. As discussed above, we are proposing to make the use and exchange of protected health information relatively easy for health care purposes and more difficult for purposes other than health care.

As a general rule, we are proposing that protected health information not be used or disclosed by covered entities except as authorized by the individual who is the subject of such information or as explicitly provided by this rule. Under this proposal, most uses and disclosures of an individual's protected health information would not require explicit authorization by the individual, but would be restricted by the provisions of the rule. Covered entities would be able to use or disclose an individual's protected health information without authorization for treatment, payment and health care operations. See proposed § 164.506(a)(1)(i). Covered entities also would be permitted to use or disclose an individual's protected health information for specified public and public policy-related purposes, including public health, research, health oversight, law enforcement, and use by coroners. Covered entities would be *permitted* by this rule to use and disclose protected health information when required to do so by other law, such as a mandatory reporting requirement under State law or pursuant to a search warrant. See proposed § 164.510. Covered entities would be *required* by this rule to disclose protected health information for only two purposes: To permit individuals to inspect and copy protected health information about them (see proposed § 164.514) and for enforcement of this rule (see proposed § 164.522(e)).

The proposed rule generally would not require covered entities to vary the level of protection of protected health information based on the sensitivity of such information. We believe that all protected health information should have effective protection from inappropriate use and disclosure by covered entities, and except for limited classes of information that are not needed for treatment and payment purposes, we have not provided additional protection to protected health information that might be considered particularly sensitive. We would note that the proposed rule would not preempt provisions of other applicable laws that provide additional privacy protection to certain classes of protected health information. We understand, however, that there are medical conditions and treatments that individuals may believe are particularly sensitive, or which could be the basis of stigma or discrimination. We invite comment on whether this rule should provide for additional protection for such information. We would appreciate comment that discusses how such information should be identified and the types of steps that covered entities could take to provide such additional protection. We also invite comment on how such provisions could be enforced.

Covered entities of all types and sizes would be required to comply with the proposed privacy standards outlined below. The proposed standards would not impose particular mechanisms or procedures that covered entities must adopt to implement the standards. Instead, we would require that each affected entity assess its own needs and devise, implement, and maintain appropriate privacy policies, procedures, and documentation to address its business requirements. How each privacy standard would be satisfied would be business decisions that each entity would have to make. This allows the privacy standards to establish a stable baseline, yet remain flexible enough to take advantage of developments and methods for protecting privacy that will evolve over time.

Because the privacy standards would need to be implemented by all covered entities, from the smallest provider to the largest, multi-state health plan, a single approach to implementing these standards would be neither economically feasible nor effective in safeguarding health information privacy. For example, in a small physician practice, the office manager might be designated to serve as the privacy official as one of many duties (see proposed § 164.518(a)) whereas at a large health plan, the privacy official may constitute a full time position and have the regular support and advice of a privacy staff or board.

Similarly, a large enterprise may make frequent electronic disclosures of similar data. In such a case, the enterprise would be expected to remove identifiers or to limit the data fields that are disclosed to fit the purpose of the disclosure. The process would be documented and perhaps even automated. A solo physician's office, however, would not be expected to have the same capabilities to limit the amount of information disclosed, although, in the cases of disclosures involving a small number of records, such an office could be expected to hide identifiers or to limit disclosures to certain pages of the medical record that are relevant to the purpose of the disclosure.

In taking this approach, we intend to strike a balance between the need to maintain the confidentiality of protected health information and the economic cost of doing so. Health care entities must consider both aspects in devising their solutions. This approach is similar to the approach we proposed in the Notice of Proposed Rulemaking for the administrative simplification security and electronic signature standards.

1. Use and Disclosure for Treatment, Payment, and Health Care Operations. (§ 164.506(a))

[*Please label comments about this section with the subject: ''Treatment, payment, and health care operations''*]

We are proposing that, subject to limited exceptions for psychotherapy notes and research information unrelated to treatment discussed below, a covered entity be permitted to use or disclose protected health information without individual authorization for treatment, payment or health care operations.

The Secretary's Recommendations proposed that covered entities be able to use individually identifiable health information without authorization of the identified individual for treatment and payment and for purposes that are ''compatible with and directly related to'' treatment and payment. The Recommendations further explained that the terms ''treatment'' and ''payment'' were to be construed broadly, encompassing treatment and payment for all patients. They also noted that the test of ''compatible with and directly related to'' is meant to be more restrictive than the test currently used in the Privacy Act, 5. U.S.C. 552a, for determining whether a proposed ''routine use'' is sufficiently related to the primary purpose for which the information would be collected to permit its release under the proposed ''routine use.'' The Privacy Act permits release of such information if the proposed routine use is ''compatible with'' the purpose for which the information is collected. Our proposal is intended to be consistent with this discussion from the Secretary's Recommendations.

a. *General rule for treatment, payment, and health care operations.* We are not proposing to require individual authorizations of uses and disclosures for health care and related purposes, although such authorizations are routinely gathered today as a condition of obtaining health care or enrolling in a health plan. Although many current disclosures of health information are made pursuant to individual authorizations, these authorizations provide individuals with little actual control over their health information. When an individual is required to sign a blanket authorization at the point of receiving care or enrolling for coverage, that consent is often not voluntary because the individual must sign the form as a condition of treatment or payment for treatment. Individuals are also often asked to sign broad authorizations but are provided little or no information about how their health information may be or will in fact be used. Individuals cannot make a truly informed decision without knowing all the possible uses, disclosures and re-disclosures to which their information will be subject. In addition, since the authorization usually precedes creation of the record, the individual cannot predict all the information the record may contain and therefore cannot make an informed decision as to what would be released.

Our proposal is intended to make the exchange of protected health information relatively easy for health care purposes and more difficult for purposes other than health care. For individuals, health care treatment and payment are the core functions of the health care system. This is what they expect their health information will be used for when they seek medical care and present their proof of insurance to the provider. Consistent with this expectation, we considered requiring a separate individual authorization for every use or disclosure of information but rejected such an approach because it would not be realistic in an increasingly integrated health care system. For example, a requirement for separate patient authorization for each routine referral could impair care, by delaying consultation and referral, as well as payment.

We therefore propose that covered entities be permitted to use and disclose protected health information without individual authorization for treatment and payment purposes, and for related purposes that we have defined as health care operations. For example, health care providers could maintain and refer to a medical record, disclose information to other providers or persons as necessary for consultation about diagnosis or treatment, and disclose information as part of referrals to other providers. Health care providers also could use a patient's protected health information for payment purposes such as submitting a claim to a payer. In addition, they could use a patient's protected health information for health care operations, such as use for an internal quality oversight review. We would note that, in the case of an individual where the provider has agreed to restrictions on use or disclosure of the patient's protected health information, the provider is bound by such restrictions as provided in § 164.506(c).

Similarly, health plans could use an enrollee's protected health information for payment purposes, such as reviewing and paying health claims that have been submitted to it, pre-admission screening of a request for hospitalization, or post-claim audits of health care providers. Health plans also could use an enrollee's protected health information for health care operations, such as reviewing the utilization patterns or outcome performance of providers participating in their network.

Further, as described in more detail below, health care providers and health plans would not need individual authorization to provide protected health information to a business partner for treatment, payment or health care operations functions if the other requirements for disclosing to business partners are met. See proposed § 164.506(e).

We intend that the right to use and disclose protected health information be interpreted to apply for treatment and payment of all individuals. For example, in the course of providing care to a patient, a physician could wish to examine the records of other patients with similar conditions. Likewise, a physician could consult the records of several people in the same family or living in the same household to assist in diagnosis of conditions that could be contagious or that could arise from a common environmental factor. A health plan or a provider could use the protected health information of a number of enrollees to develop treatment protocols, practice guidelines, or to assess quality of care. All of these uses would be permitted under this proposed rule.

Our proposal would not restrict to whom disclosures could be made for treatment, payment or operations. For example, covered entities could make disclosures to non-covered entities for payment purposes, such as a disclosure to a workers compensation carrier for coordination of benefits purposes. We note, however, that when disclosures are made to non-covered entities, the ability of this proposed rule to protect the confidentiality of the information ends. This points to the need for passage of more comprehensive privacy legislation that would permit the restrictions on use and disclosure to follow the information beyond covered entities.

We also propose to prohibit covered entities from seeking individual authorization for uses and disclosures for treatment, payment and health care operations unless required by State or other applicable law. As discussed above in this section, such authorizations could not provide meaningful privacy protections or individual control and could in fact cultivate in individuals erroneous understandings of their rights and protections.

The general approach that we are proposing is not new. Some existing State health confidentiality laws permit disclosures without individual authorization to other health care providers treating the individual, and the Uniform Health-Care Information Act permits disclosure ''to a person who is providing health-care to the patient'' (9 part I, U.L.A. 475, 2–104 (1988 and Supp. 1998)). We believe that this approach would be the most realistic way to protect individual confidentiality in an increasingly data-driven, electronic and integrated health care system. We recognize, however, that particularly given the limited scope of the authority that we have under this proposed rule to reach some significant actors in the health care system, that other approaches could be of interest. We invite comments on whether other approaches to protecting individuals' health information would be more effective.

b. *Health care operations.* We considered the extent to which the covered entities might benefit from further guidance on the types of activities that appropriately would be considered health care operations. The term is defined in proposed § 164.504. In the debates that have surrounded privacy legislation before the Congress, there has been substantial discussion of the definition of health care operations, with some parties advocating for a very broad definition and others advocating a more restrictive approach.

Given the lack of consensus over the extent of the activities that could be encompassed within the term health care operations, we determined that it would be helpful to identify activities that, in our opinion, are sufficiently unrelated to the treatment and payment functions to require a individual to authorize use of his or her information. We want to make clear that these activities would not be prohibited, and do not dispute that many of these activities are indeed beneficial to both individuals and the institutions involved. Nonetheless, they are not necessary for the key functions of treatment and payment and therefore would require the authorization of the individual before his/her information could be used. These activities would include but would not be limited to:

- The use of protected health information for marketing of health and non-health items and services;
- The disclosure of protected health information for sale, rent or barter;
- The use of protected health information by a non-health related division of the same corporation, e.g., for use in marketing or underwriting life or casualty insurance, or in banking services;
- The disclosure, by sale or otherwise, of protected health information to a plan or provider for making eligibility or enrollment determinations, or for underwriting or risk rating determinations, prior to the individual's enrollment in the plan;
- The disclosure of information to an employer for use in employment determinations; and
- The use or disclosure of information for fund raising purposes.

We invite comments on the activities within the proposed definitions of ''treatment,'' ''payment,'' and ''health care operations,'' as well as the activities proposed to be excluded from these definitions.

c. *Exception for psychotherapy notes.* We propose that a covered health care provider not be permitted to disclose psychotherapy notes, as defined by this proposed rule, for treatment, payment, or health care operations unless a specific authorization is obtained from the individual. In addition, a covered entity would not be permitted to condition treatment of an individual, enrollment of an individual in a health plan, or payment of a claim for benefits made by or on behalf of an individual on a requirement that the individual provide a specific authorization for the disclosure of psychotherapy notes.

We would define ''psychotherapy notes'' to mean detailed notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session. Such notes could be used only by the therapist who wrote them, would have to be maintained separately from the medical record, and could not be involved in the documentation necessary for health care treatment, payment, or operations (as defined in § 164.504). Such term would not include medication prescription and monitoring, counseling session start and stop times or the modalities and frequencies of treatment furnished, results of clinical tests, or summaries of the following items: diagnoses, functional status, the treatment plan, symptoms, prognosis and progress to date.

Psychotherapy notes are of primary value to the specific provider and the promise of strict confidentiality helps to ensure that the patient will feel comfortable freely and completely disclosing very personal information essential to successful treatment. Unlike information shared with other health care providers for the purposes of treatment, psychotherapy notes are more detailed and subjective and are subject to unique rules of disclosure. In *Jaffee* v. *Redmond,* 518 U. S. 1 (1996), the Supreme Court ruled that conversations and notes between a patient and psychotherapist are confidential and protected from compulsory disclosure. The language in the Supreme Court opinion makes the rationale clear:

> Like the spousal and attorney-client privileges, the psychotherapist-patient privilege is ''rooted in the imperative need for confidence and trust.'' * * * Treatment by a physician for physical ailments can often proceed successfully on the basis of a physical examination, objective information supplied by the patient, and the results of diagnostic tests. Effective psychotherapy, by contrast, depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fears. Because of the sensitive nature of the problems for which individuals consult psychotherapists, disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason, the mere possibility of disclosure may impede development of the confidential relationship necessary for successful treatment. As the Judicial Conference Advisory Committee observed in 1972 when it recommended that Congress recognize a psychotherapist privilege as part of the Proposed Federal Rules of Evidence, a psychiatrist's ability to help her patients ''is completely dependent upon (the patients') willingness and ability to talk freely. This makes it difficult if not impossible for (a psychiatrist) to function without being able to assure * * * patients of confidentiality and, indeed, privileged communication. Where there may be exceptions to this general rule * * *, there is wide agreement that confidentiality is a *sine qua non* for successful psychiatric treatment. * * *''

By protecting confidential communications between a psychotherapist and her patient from involuntary disclosure, the proposed privilege thus serves important private interests. * * * The psychotherapist privilege serves the public interest by facilitating the provision of 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.

That it is appropriate for the federal courts to recognize a psychotherapist privilege under Rule 501 is confirmed by the fact that all 50 States and the District of Columbia have enacted into law some form of psychotherapist privilege. * * * Because state legislatures are fully aware of the need to protect the integrity of the fact finding functions of their courts, the existence of a consensus among the States indicates that ''reason and experience'' support recognition of the privilege. In addition, given the importance of the patient's understanding that her communications with her therapist will not be publicly disclosed, any State's promise of confidentiality would have little value if the patient were aware that the privilege would not be honored in a federal court. * * * *Jaffee,* 518 U.S. 7–9.

The special status of the psychotherapist privilege in our society as well as the physical and conceptual segregation of the psychotherapy notes makes this prohibition on disclosures for treatment, payment and health care operations without a specific authorization from the individual reasonable and practical.

We note that the policy being applied to psychotherapy notes differs from the policy being applied to most other types of protected health information. For most protected health information, a covered entity would be prohibited from soliciting an authorization from an individual for treatment, payment and health operations unless such an authorization is required by other applicable law. In this case, because of the special status of psychotherapy notes as described above, we propose that a specific authorization be required before such notes can be disclosed within the treatment and payment systems. We propose this special treatment because there are few reasons why other health care entities should need the psychotherapy notes about an individual, and in those cases, the individual is in the best position to determine if the notes should be disclosed. For example, an individual could authorize disclosure if they are changing health care providers. Since we have defined psychotherapy notes in such a way that they do not include information that health plans would need to process a claim for services, special authorizations for payment purposes should be rare. We would note that the provisions governing authorizations under § 164.508 would apply to the special authorizations under this provision.

We also propose that covered entities not be permitted to condition treatment or payment decisions on a requirement that an individual provide a specific authorization for the use or disclosure of psychotherapy notes. The special protections that are being proposed would not be meaningful if covered entities could coerce individuals by conditioning treatment or payment decisions on a requirement that the individual authorize use or disclosures of such notes. This requirement would not prohibit the provider that creates the psychotherapy notes information from using the notes for treatment of the individual. The provider could not, however, condition the provision of treatment on a requirement that the individual authorize the use of the psychotherapy notes by the covered entity for other purposes or the disclosure of the notes by the provider to others.

We considered including other disclosures permitted under proposed § 164.510 within the prohibition described in this provision, but were unsure if psychotherapy notes were ever relevant to the public policy purposes underlying those disclosures. For example, we would assume that such notes are rarely disclosed for public health purposes or to next of kin. We solicit comment on whether there are additional categories of disclosures permitted under proposed § 164.510 for which the disclosure of psychotherapy notes by covered entities without specific individual authorization would be appropriate.

d. *Exception for research information unrelated to treatment.* Given the voluntary, often altruistic, nature of research participation, and the experimental character of data generated from many research studies, research participants should have assurances that the confidentiality of their individually identifiable information will be maintained in a manner that respects these unique characteristics. In the process of conducting health research, some information that is collected could be related to the delivery of health care to the individual and some could be unrelated to the care of the individual. Some information that is generated in the course of a research study could have unknown analytic validity, clinical validity, or clinical utility. In general, unknown analytic or clinical validity means that the sensitivity, specificity, and predictive value of the research information is not known. Specifically, analytic validity refers to how well a test performs in measuring the property or characteristic it is intended to measure. Another element of the test's analytical validity is its reliability—that is, it must give the same result each time. Clinical validity is the accuracy with which a test predicts a clinical condition. Unknown clinical utility means that there is an absence of scientific and medical agreement regarding the applicability of the information for the diagnosis, prevention, or treatment of any malady, or the assessment of the health of the individual.

We would define ''research information unrelated to treatment'' as information that is received or created by a covered entity in the course of conducting research for which there is insufficient scientific and medical evidence regarding the validity or utility of the information such that it should not be used for the purpose of providing health care, and with respect to which the covered entity has not requested payment from a health plan.

Such information should never be used in a clinical treatment protocol but could result as a byproduct of such a protocol. For example, consider a study which involves the evaluation of a new drug, as well as an assessment of a genetic marker. The drug trial includes physical and radiographic examinations, as well as blood tests to monitor potential toxicity of the new drug on the liver; all of these procedures are part of the provision of health care, and therefore, would constitute ''protected health information,'' but not ''research information unrelated to treatment.'' In the same study, the investigators are searching for a genetic marker for this particular disease. To date, no marker has been identified and it is uncertain whether or not the preliminary results from this research study would prove to be a marker for this disease. The genetic information generated from this study would constitute ''research information unrelated to treatment''.

We solicit comment on this definition of ''research information unrelated to treatment'' and how it would work in practice.

Because the meaning of this information is currently unknown, we would prohibit its use and disclosure for treatment, payment and health care operations unless a specific authorization is obtained from the subject of the information. Failing to limit the uses and disclosures of this information within the health payment system would place research participants at increased risk of discrimination, which could result in individuals refusing to volunteer to participate in this type of research. Without the special protections that we are proposing, we are concerned that much potentially life-saving research could be halted. Moreover, because this information that lacks analytical or clinical validity and clinical utility, and because we have defined it in terms that preclude researchers from seeking third-party reimbursement for its creation, there would not be a reason for this information to be further used or disclosed within the treatment and payment system without individual authorization.

We also propose that covered entities not be permitted to condition treatment or payment decisions on a requirement that an individual provide a specific authorization for the use or disclosure of research information unrelated to treatment. The special protections that are being proposed would not be meaningful if covered entities could coerce individuals into authorizing disclosure by conditioning treatment or payment decisions on a requirement that the individual authorize disclosures of such information. This requirement would not prohibit the covered entity that creates the information from using the information for the research purposes for which it was collected. The entity could not, however, condition the provision of treatment on a requirement that the individual authorize use of research information unrelated to treatment by the covered entity for other purposes or the disclosure of the information by the covered entity to others.

We considered including other of the uses and disclosures that would be permitted under § 164.510 within the prohibition described in this provision, but were unsure if research information unrelated to treatment would ever be relevant to the public policy purposes underlying those disclosures. We solicit comment on whether there are additional categories of uses or disclosures that would be permitted under proposed § 164.510 for which the use or disclosure of such information by covered entities without specific individual authorization would be appropriate.

2. Minimum Necessary Use and Disclosure. (§ 164.506(b))

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

We propose that, except as discussed below, a covered entity must make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose of the use or disclosure, taking into consideration practical and technological limitations.

In certain circumstances, the assessment of what is minimally necessary is appropriately made by a person other than the covered entity; in those cases, discussed in this paragraph, and reflected in proposed § 164.506(b)(1)(i), the requirements of this section would not apply. First, the covered entity would not be required to make a ''minimum necessary'' analysis for the standardized content of the various HIPAA transactions, since that content has been determined through regulation. Second, with one exception, when an individual authorizes a use or disclosure the covered entity would not be required to make a ''minimum necessary'' determination. In such cases, the covered entity would be unlikely to know enough about the information needs of the third party to make a ''minimum necessary'' determination. The exception, when the ''minimum necessary'' principle would apply to an authorization, is for authorizations for use of protected health information by the covered entity itself. See proposed § 164.508(a)(2). Third, with respect to disclosures that are mandatory under this or other law, and which would be permitted under the rules proposed below, public officials, rather than the covered entity, would determine what information is required (e.g., coroners and medical examiners, State reporting requirements, judicial warrants). See proposed §§ 164.510 and 164.506(b)(1)(ii). Fourth, disclosure made pursuant to a request by the individual for access to his or her protected health information presents no possible privacy threat and therefore lies outside this requirement. See proposed § 164.506(b)(1)(i).

Under this proposal, covered entities generally would be required to establish policies and procedures to limit the amount of protected health care information used or disclosed to the minimum amount necessary to meet the purpose of the use or disclosure, and to limit access to protected health information only to those people who need access to the information to accomplish the use or disclosure. With respect to use, if an entity consists of several different components, the entity would be required to create barriers between components so that information is not used inappropriately. For example, a health plan that offers other insurance products would have policies and procedures to prevent protected health information from crossing over from one product line to another. The same principle applies to disclosures. For example, if a covered entity opts to disclose protected health information to a researcher pursuant to proposed § 164.510(j), it would need to ensure that only the information necessary for the particular research protocol is disclosed.

It should be noted that, under section 1173(d) of the Act, covered entities would also be required to satisfy the requirements of the Security standards, by establishing policies and procedures to provide access to health information systems only to persons who require access, and implement procedures to eliminate all other access. Thus, the privacy and security requirements would work together to minimize the amount of information shared, thereby lessening the possibility of misuse or inadvertent release.

A ''minimum necessary'' determination would need to be consistent with and directly related to the purpose of the use or disclosure and take into consideration the ability of a covered entity to delimit the amount of information used or disclosed and the relative burden imposed on the entity. The proposed minimum necessary requirement is based on a reasonableness standard: covered entities would be required to make reasonable efforts and to incur reasonable expense to limit the use and disclosure of protected health information as provided in this section.

In determining what a reasonable effort is under this section, covered entities should take into consideration the amount of information that would be used or disclosed, the extent to which the use or disclosure would extend the number of individuals or entities with access to the protected health information, the importance of the use or disclosure, the likelihood that further uses or disclosures of the protected health information could occur, the potential to achieve substantially the same purpose with de-identified information, the technology available to limit the amount of protected health information that is used or disclosed, the cost of limiting the use or disclosure, and any other factors that the covered entity believes are relevant to the determination. We would expect that in most cases where covered entities have more information than is necessary to accomplish the purpose of a use or disclosure, some method of limiting the information that is used or disclosed could be found.

We note that all of the uses and disclosures subject to the requirements of this provision are permissive; the minimum necessary provision does not apply to uses or disclosures mandated by law. Covered entities should not make uses or disclosures of protected health information where they are unable to make any efforts to reasonably limit the amount of protected health information used or disclosed for a permissive purpose. Where there is ambiguity regarding the particular information to be used or disclosed, this provision should be interpreted to require the covered entity or make some effort to limit the amount of information used or disclosed.

We note that procedures for implementing the minimum necessary requirement for uses would often focus on limiting the physical access that employees, business partners and others would have to the protected health information. Procedures which limit the specific employees or business partners, or the types of employees or business partners, who would be qualified to gain access to particular records would often be appropriate. Covered entities with advanced technological capabilities should also consider limiting access to appropriate portions of protected health information when it would be practical to do so.

The ''minimum necessary'' determination would include a determination that the purpose of the use or disclosure could not be reasonably accomplished with information that is not identifiable. Each covered entity would be required to have policies for determining when information must be stripped of identifiers before disclosure. If identifiers are not removed simply because of inconvenience to the covered entity, the ''minimum necessary'' rule would be violated.

Similarly, disclosure of an entire medical record, in response to a request for something other than the entire medical record, would presumptively violate the ''minimum necessary'' rule. Except where the individual has specifically authorized use or disclosure of the full medical record, when a covered entity receives a request for an entire medical record, the covered entity could not, under these proposed rules, disclose the entire record unless the request included an explanation of why the purpose of the disclosure could not reasonably be accomplished without the entire medical record.

The decisions called for in determining what would be the minimum necessary information to accomplish an allowable purpose should include both a respect for the privacy rights of the subjects of the medical record and the reasonable ability of covered entities to delimit the amount of individually identifiable health information in otherwise permitted uses and disclosures. For example, a large enterprise that makes frequent electronic disclosures of similar data would be expected to remove identifiers or to limit the data fields that are disclosed to fit the purpose of the disclosure. An individual physician's office would not be expected to have the same capabilities to limit the amount of information disclosed, although, in the cases of disclosures involving a small number of records, such an office could be expected to hide identifiers or to limit disclosures to certain pages of the medical record that are relevant to the purpose of the disclosure.

Even where it might not be reasonable for a covered entity to limit the amount of information disclosed, there could be opportunities, when the use or disclosure does not require authorization by the individual, to reduce the scope of the disclosure in ways that substantially protect the privacy interests of the subject. For example, if a health researcher wants access to relatively discrete parts of medical records that are presently maintained in paper form for a large number of patients with a certain condition, it could be financially prohibitive for the covered entity to isolate the desired information. However, it could be reasonable for the covered entity to allow the researcher to review the records on-site and to abstract only the information relevant to the research. Much records research is done today through such abstracting, and this could be a good way to meet the ''minimum necessary'' principle. By limiting the physical distribution of the record, the covered entity would have effectively limited the scope of the disclosure to the information necessary for the purpose.

Proposed § 164.506(b) generally would place the responsibility for determining what disclosure is the ''minimum necessary'' on the covered entity making the disclosure. The exception would be for health plan requests for information from health care providers for auditing and related purposes. In this instance, since the provider is not in a position to negotiate with the payer, the duty would be shifted to the payer to request the ''minimum necessary'' information for the purpose. See proposed § 164.506(b)(1)(iv). Whenever a health plan requests a disclosure, it would be required to limit its requests to the information to achieve the purpose of the request. For example, a health plan seeking protected health information from a provider or other health plan to process a payment should not request the entire health record unless it is actually necessary.

In addition, the proposal would permit covered entities to reasonably rely on requests by certain public agencies in determining the minimum necessary information for certain disclosures. For example, a covered entity that reasonably relies on the requests of public health agencies, oversight agencies, law enforcement agencies, coroners or medical examiners would be in compliance with this requirement. See proposed § 164.506(b)(3).

As discussed in prior HIPAA proposed rulemakings, it is likely to be easier to limit disclosure when disclosing computerized records than when providing access to paper records. Technological mechanisms to limit the amount of information available for a particular purpose, and make information available without identifiers, are an important contribution of technology to personal privacy. For example, the fields of information that are disclosed can be limited, identifiers (including names, addresses and other data) can be removed, and encryption can restrict to authorized personnel the ability to link identifiers back to the record.

For electronic information covered by the proposed rules, the ''minimum necessary'' requirement would mean reviewing, forwarding, or printing out only those fields and records relevant to the user's need for information. Where reasonable (based on the size, sophistication and volume of the covered entity's electronic information systems), covered entities would configure their record systems to allow selective access to different portions of the record, so that, for example, administrative personnel get access to only certain fields, and medical personnel get access to other fields. This selective access to information would be implemented using the access control technology discussed in the electronic security regulation.

For non-electronic information covered by the proposed rules, ''minimum necessary'' would mean the selective copying of relevant parts of protected health information or the use of ''order forms'' to convey the relevant information. These techniques are already in use in the health care environment today, not because of privacy considerations, but because of the risk of losing access to the full medical record when needed for clinic or emergency visits.

This rule would require, in proposed § 164.520, that each covered entity document the administrative policies and procedures that it will use to meet the requirements of this section. With respect to the ''minimum necessary'' compliance standard, such procedures would have to describe the process or processes by which the covered entity will make minimum necessary determinations, the person or persons who will be responsible for making such determinations, and the process in place to periodically review routine uses and disclosures in light of new technologies or other relevant changes. Proposed uses or disclosures would have to be reviewed by persons who have an understanding of the entity's privacy policies and practices, and who have sufficient expertise to understand and weigh the factors described above. See proposed § 164.506(b)(2). The policies that would be reasonable would vary depending on the nature and size of the covered entity. For large enterprises, the documentation of policies and procedures might identify the general job descriptions of the people that would make such decisions throughout the organization.

In addition, the procedures would provide that the covered entity will review each request for disclosure individually on its own merits (and, for research, the documentation of required IRB or other approval). Covered entities should not have general policies of approving all requests (or all requests of a particular type) for disclosures or uses without carefully considering the factors identified above as well as other information specific to the request that the entity finds important to the decision.

We understand that the requirements outlined in this section do not create a bright line test for determining the minimum necessary amount of protected health information appropriate for most uses or disclosures. Because of this lack of precision, we considered eliminating the requirement altogether. We also considered merely requiring covered entities to address the concept within their internal privacy procedures, with no further guidance as to how each covered entity would address the issue. These approaches were rejected because minimizing both the amount of protected health information used and disclosed within the health care system and the number of persons who have access to such information is vital if we are to successfully enhance the confidentiality of people's personal health information. We invite comments on the approach that we have adopted and on alternative methods of implementing the minimum necessary principle.

3. Right to Restrict Uses and Disclosures. (§ 164.506(c))

[*Please label comments about this section with the subject: ''Right to restrict''*]

We propose to permit in § 164.506(c) that individuals be able to request that a covered entity restrict further uses and disclosures of protected health information for treatment, payment, or health care operations, and if the covered entity agrees to the requested restrictions, the covered entity could not make uses or disclosures for treatment, payment or health care operations that are inconsistent with such restrictions, unless such uses or disclosures are mandated by law. This provision would not apply to health care provided to an individual on an emergency basis.

This proposal would not restrict the right of a provider to make an otherwise permissible disclosure under § 164.510, such as a disclosure for public health or emergency purposes. While there is nothing in this proposed rule that would prohibit a provider and an individual from agreeing in advance not to make such disclosures, such an agreement would not be enforceable through this proposed rule.

We should note that there is nothing in this proposed rule that requires a covered entity to agree to a request to restrict, or to treat or provide coverage to an individual requesting a restriction under this provision. Covered entities who do not wish to, or due to contractual obligations cannot, restrict further use or disclosure would not be obligated to treat an individual making a request under this provision. For example, some health care providers could feel that it is medically inappropriate to honor patient requests under this provision. The medical history and records of a patient, particularly information about current medications and other therapies, are often very much relevant when new treatment is sought, and the patient cannot seek to withhold this information from subsequent providers without risk.

Under this proposal, individuals could request broad restrictions on further uses and disclosures for treatment, payment or health care operations, or could request more limited restrictions relating to further uses or disclosures of particular portions of the protected health information or to further disclosures to particular persons. Covered entities could choose to honor the individual's request, could decline to treat or provide coverage to the individual, or could propose an alternative restriction of further use or disclosure. The covered entity would not be bound by an individual's request for restriction until its scope has been agreed to by the individual and the provider. Once an agreement has been reached, however, a covered entity that uses or discloses the protected health information resulting from the encounter in any manner that violates such agreement would be in violation of this provision.

We are not proposing to extend this right to individuals receiving emergency medical care, because emergency situations may not afford sufficient opportunity for the provider and patient to discuss the potential implications of restricting further use and disclosure of the resulting medical information. Additionally, a health care provider may not be free to refuse treatment to an emergency patient if the provider does not wish to honor a request to restrict further use or disclosure of health information, leaving the provider in an unfair position where she or he must choose between permitting medical harm to come to the patient or honoring a request that she or he feels may be inappropriate or which may violate the provider's business practices or contractual obligations. Some health care providers are legally required to treat emergency patients (e.g., hospital emergency rooms), and would have no opportunity to refuse treatment as a result of a request to restrict further use and disclosure under this provision. Under the pressure of an emergency, a provider should not be expected to adhere to the restrictions associated with a particular individual's information.

Under this proposal, covered entities would not be responsible for ensuring that agreed-upon restrictions are honored when the protected health information leaves the control of the covered entity or its business partners. For example, a provider would not be out of compliance if information she or he disclosed to another provider (consistent with the agreed upon restrictions and with notice of the applicable restrictions on uses and disclosures) is subsequently used or disclosed in violation of the restrictions.

The agreement to restrict use and disclosure under this provision would have to be documented to be binding on the covered entity. In proposed § 164.520, we would require covered entities to develop and document policies and procedures reasonably designed to ensure that the requests are followed, i.e., that unauthorized uses and disclosures are not made.

We note that this proposed rule would not permit covered entities to require individuals to invoke their right to restrict uses and disclosures; only the patient could make a request and invoke this right to restrict.

We considered providing individuals substantially more control over their protected health information by requiring all covered entities to attempt to accommodate any restrictions on use and disclosure requested by patients. We rejected this option as unworkable. While industry groups have developed principles for requiring patient authorizations, we have not found widely accepted standards for implementing patient restrictions on uses or disclosures. Restrictions on information use or disclosure contained in patient consent forms are sometimes ignored because they may not be read or are lost in files. Thus, it seems unlikely that a requested restriction could successfully follow a patient's information through the health care system—from treatment to payment, through numerous operations, and potentially through certain permissible disclosures. Instead we would limit the provision to restrictions that have been agreed to by the covered entity.

We recognize that the approach that we are proposing could be difficult because of the systems limitations described above. However, we believe that the limited right for patients included in this proposed rule can be implemented because it only applies in instances in which the covered entity agrees to the restrictions. We assume that covered entities would not agree to restrictions that they are unable to implement.

We considered limiting the rights under this provision to patients who pay for their own health care (or for whom no payment was made by a health plan). Individuals and health care providers that engage in self-pay transactions have minimal effect on the rights or responsibilities of payers or other providers, and so there would be few instances when a restriction agreed to in such a situation would have negative implications for the interests of other health care actors. Limiting the right to restrict to self-pay patients also would reduce the number of requests that would be made under this provision. We rejected this approach however, because the desire to restrict further uses and disclosures arises in many instances other than self-pay situations. For example, a patient could request that his or her records not be shared with a particular physician because that physician is a family friend. Or an individual could be seeking a second opinion and might not want his or her treating physician consulted. Individuals have a legitimate interest in restricting disclosures in these situations. We solicit comment on the appropriateness of limiting this provision to instances in which no health plan payment is made on behalf of the individual.

In making this proposal, we recognize that it could be difficult in some instances for patients to have a real opportunity to make agreements with covered entities, because it would not be clear in all cases which representatives of a covered entity could make an agreement on behalf of the covered entity. There also are concerns about the extent to which covered entities could ensure that agreed-upon restrictions would be followed. As mentioned above, current restrictions contained in patient consent forms are sometimes ignored because the person handling the information is unaware of the restrictions. We solicit comments on the administrative burdens this provision creates for covered entities, such as the burdens of administering a system in which some information is protected by federal law and other information is not.

We would note that we expect that systems for handling patient requests to restrict use and disclosure of information will become more responsive as technology develops. Therefore, we will revisit this provision as what is practicable changes over time. Proposed requirements for documenting internal procedures to implement this proposed provision are included in proposed § 164.520. We request comments on whether the final rule should provide examples of appropriate, scalable systems that would be in compliance with this standard.

4. Creation of De-identified Information (164.506(d))

[*Please label comments about this section with the subject: ''Creation of de-identified information''*]

In this rule we are proposing that covered entities and their business partners be permitted to use protected health information to create de-identified health information. Covered entities would be permitted to further use and disclose such de-identified information in any way, provided that they do not disclose the key or other mechanism that would enable the information to be re-identified, and provided that they reasonably believe that such use or disclosure of de-identified information will not result in the use or disclosure of protected health information. See proposed § 164.506(d)(1). This means that a covered entity could not disclose de-identified information to a person if the covered entity reasonably believes that the person would be able to re-identify some or all of that information, unless disclosure of protected health information to such person would be permitted under this proposed rule. In addition, a covered entity could not use or disclose the key to coded identifiers if this rule would not permit the use or disclosure of the identified information to which the key pertains. If a covered entity re-identifies the de-identified information, it may only use or disclose the re-identified information consistent with these proposed rules, as if it were the original protected health information.

In some instances, covered entities creating de-identified health information could want to use codes or identifiers to permit data attributable to the same person to be accumulated over time or across different sources of data. For example, a covered entity could automatically code all billing information as it enters the system, substituting personal identifiers with anonymous codes that permit tracking and matching of data but do not permit people handling the data to create protected health information. Such a mechanism would be permissible as long as the key to unlocking the codes is not available to the people working with the de-identified information, and the entity otherwise makes no attempt to create protected health information from the de-identified information.

There are many instances in which such individually identifiable health information is stripped of the information that could identify individual subjects and is used for analytical, statistical and other related purposes. Large data sets of de-identified information can be used for innumerable purposes that are vital to improving the efficiency and effectiveness of health care delivery, such as epidemiological studies, comparisons of cost, quality or specific outcomes across providers or payers, studies of incidence or prevalence of disease across populations, areas or time, and studies of access to care or differing use patterns across populations, areas or time. Researchers and others often obtain large data sets with de-identified information from providers and payers (including from public payers) to engage in these types of studies. This information is valuable for public health activities (e.g., to identify cost-effective interventions for a particular disease) as well as for commercial purposes (e.g., to identify areas for marketing new health care services).

We intend that this proposed provision will permit the important health care research that is being conducted today to continue under this rule. Indeed, it would be our hope that covered entities, their business partners, and others would make greater use of de-identified health information than they do today, when it is sufficient for the research purpose. Such practice would reduce the confidentiality concerns that result from the use of individually identifiable health information for some of these purposes. The selective transfer of health information without identifiers into an analytic database would significantly reduce the potential for privacy violations while allowing broader access to information for analytic purposes, without the overhead of audit trails and IRB review. For example, providing de-identified information to a pharmaceutical manufacturer to use in determining patterns of use of a particular pharmaceutical by general geographic location would be appropriate, even if the information were sold to the manufacturer. Such analysis using protected health information would be research and therefore would require individual authorization or approval by an IRB or similar board. We note that data that includes an individual's address is ''identifiable'' by definition and could not be used in such databases.

We invite comment on the approach that we are proposing and on whether alternative approaches to standards for entities determining when health information can reasonably be considered no longer individually identifiable.

5. Application to business partners. (§ 164.506(e))

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

In § 164.506(e), we propose to require covered entities to take specific steps to ensure that protected health information disclosed to a business partner remains protected. We intend these provisions to allow customary business relationships in the health care industry to continue while providing privacy protections to the information shared in these relationships. Business partners would not be permitted to use or disclose protected health information in ways that would not be permitted of the covered entity itself under these rules.

Other than for purposes of consultation or referral for treatment, we would allow covered entities to disclose protected health information to business partners only pursuant to a written contract that would, among other specified provisions, limit the business partner's uses and disclosures of protected health information to those permitted by the contract, and would impose certain security, inspection and reporting requirements on the business partner. We would hold the covered entity responsible for certain violations of this proposed rule made by their business partners, and require assignment of responsibilities when a covered entity acts as a business partner of another covered entity.

a. *Who is a business partner?* Under this proposed rule, a business partner would be a person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. This would include contractors or other persons who receive protected health information from the covered entity (or from another business partner of the covered entity) for the purposes described in the previous sentence, including lawyers, auditors, consultants, third-party administrators, health care clearinghouses, data processing firms, billing firms, and other covered entities. This would not include persons who would be members of the covered entity's workforce. The key features of the relationship would be that the business partner is performing an activity or function for or on behalf of the covered entity and that the business partner receives protected health information from the covered entity as part of providing such activity or function.

Many critical functions are performed every day by individuals and organizations that we would define as business partners. Under the proposal, billing agents, auditors, third-party administrators, attorneys, private accreditation organizations, clearinghouses, accountants, data warehouses, consultants and many other actors would be considered business partners of a covered entity. Most covered entities will use one or more business partners, to assist with functions such as claims filing, claims administration, utilization review, data storage, or analysis. For example, if a covered entity seeks accreditation from a private accreditation organization and provides such organization with protected health information as part of the accreditation process, the private accreditation organization would be a business partner of the covered entity. This would be true even if a third party, such as an employer or a public agency, required accreditation as a condition of doing business with it. The accreditation is being performed for the covered entity, not the third party, in such cases.

The covered entity may have business relationships with organizations that would not be considered to be business partners because protected health information is not shared or because services are not provided to the covered entity. For example, a covered entity could contract with another organization for facility management or food services; if these organizations do not receive protected health information for these functions or activities, they would not be considered business partners. In the case where a covered entity provides management services to another organization, the other organization would not be a business partner because it would be receiving, not providing, a service or function.

Under the proposal, a covered entity could become a business partner of another covered entity, such as when a health plan acts as a third-party administrator to an insurance arrangement or a self-funded employee benefit plan. In such cases, we propose that the authority of the covered entity acting as a business partner to use and disclose protected health information be constrained to the authority that any business partner in the same situation would have. Thus, the authority of a covered entity acting as a business partner to use and disclose protected health information obtained as a business partner would be limited by the contract or arrangement that created the business partner relationship.

In most cases, health care clearinghouses would fall under our definition of ''business partner'' because they receive protected health information in order to provide payment processing and other services to health plans, health care providers and their business partners, a case that would fall under our definition of ''business partner.'' Therefore, although health care clearinghouses would be covered entities, in many instances under this proposed rule they would also be treated as business partners of the health care providers or health plans for whom they are performing a service. We would note that because health care clearinghouses would generally be operating as business partners, we are proposing not to apply several requirements to health care clearinghouses that we otherwise would apply to covered plans and providers, such as requiring a notice of information practices, access for inspection and copying, and accommodation of requests for amendment or correction. See proposed §§ 164.512, 164.514 and 164.516.

b. *Limitations on use or disclosure.*

i. *Scope of the covered entity's authority.*

Under this proposed rule, a business partner would be acting on behalf of a covered entity, and we propose that its use or disclosure of protected health information be limited to the same extent that the covered entity for whom they are acting would be limited. Thus, a business partner could have no more authority to use or disclose protected health information than that possessed by the covered entity from which the business partner received the information. For example, a business partner could not sell protected health information to a financial services firm without individual authorization because the covered entity would not be permitted to do so under these proposed rules. We would note that a business partner's authority to use and disclose protected health information could be further restricted by its contract with a covered entity, as described below.

We are not proposing to require the business partners of covered entities to develop and distribute a notice of information practices, as provided in proposed § 164.512. A business partner would, however, be bound by the terms of the notice of the covered entity from which it obtains protected health information. For example, if a covered entity provided notice to its subscribers that it would not engage in certain permissible disclosures of protected health information, we are proposing that such a limitation would apply to all of the business partners of the covered entity that made the commitment. See proposed § 164.506(e). We are proposing this approach so that individuals could rely on the notices that they receive from the covered entities to which they disclose protected health information. If the business partners of a covered entity were able to make wider use or make more disclosures than the covered entity, the patients or enrollees of the covered entity would have difficulty knowing how their information was being used and to whom it was being disclosed.

ii. *Scope of the contractual agreement.*

We are also proposing that a business partner's use and disclosure of protected health information be limited by the terms of the business partner's contractual agreement with the covered entity. We propose that a contract between a covered entity and a business partner could not grant the business partner authority to make uses or disclosures of protected health information that the covered entity itself would not have the authority to make. The contract between a covered entity and a business partner could further limit the business partner's authority to use or disclose protected health information as agreed to by the parties. Further, the business partner would have to apply the same limitations to its subcontractors (or persons with similar arrangements) who assist with or carry out the business partner's activities.

To help ensure that the uses and disclosures of business partners would be limited to those recognized as appropriate by the covered entities from whom they receive protected health information, subject to the exception discussed below, we are proposing that covered entities be prohibited from disclosing protected health information to a business partner unless the covered entity has entered into a written contract with the business partner that meets the requirements of this subsection. See proposed § 164.506(e)(2)(i). The written contract between a covered entity and a business partner would be required to:

- Prohibit the business partner from further using or disclosing the protected health information for any purpose other than the purpose stated in the contract.
- Prohibit the business partner from further using or disclosing the protected health information in a manner that would violate the requirements of this proposed rule if it were done by the covered entity. As discussed above, the covered entity could not permit the business partner to make uses or disclosures that the covered entity could not make.
- Require the business partner to maintain safeguards as necessary to ensure that the protected health information is not used or disclosed except as provided by the contract. We are only proposing a general requirement; the details can be negotiated to meet the particular needs of each arrangement. For example, if the business partner is a two-person firm the contractual provisions regarding safeguards may focus on controlling physical access to a computer or file drawers, while a contract with a business partner with 500 employees would address use of electronic technologies to provide security of electronic and paper records.
- Require the business partner to report to the covered entity any use or disclosure of the protected health information of which the business partner becomes aware that is not provided for in the contract.
- Require the business partner to ensure that any subcontractors or agents to whom it provides protected health information received from the covered entity will agree to the same restrictions and conditions that apply to the business partner with respect to such information.
- Establish how the covered entity would provide access to protected health information to the subject of that information, as would be required under § 164.514, when the business partner has made any material alteration in the information. The covered entity and the business partner would determine in advance how the covered entity would know or could readily ascertain, when a particular individual's protected health information has been materially altered by the business partner, and how the covered entity could provide access to such information.
- Require the business partner to make available its internal practices, books and records relating to the use and disclosure of protected health information received from the covered entity to HHS or its agents for the purposes of enforcing the provisions of this rule.
- Establish how the covered entity would provide access to protected health information to the subject of that information, as would be required under § 164.514, in circumstances where the business partner will hold the protected health information and the covered entity will not.
- Require the business partner to incorporate any amendments or corrections to protected health information when notified by the covered entity that the information is inaccurate or incomplete.
- At termination of the contract, require the business partner to return or destroy all protected health information received from the covered entity that the business partner still maintains in any form to the covered entity and prohibit the business partner from retaining such protected health information in any form.
- State that individuals who are the subject of the protected health information disclosed are intended to be third party beneficiaries of the contract.
- Authorize the covered entity to terminate the contract, if the covered entity determines that the business partner has repeatedly violated a term of the contract required by this paragraph.

Each specified contract term above would be considered a separate implementation specification under this proposal for situations in which a contract is required, and, as discussed below, a covered entity would be responsible for assuring that each such implementation standard is met by the business partner. See proposed § 164.506(e)(2). The contract could include any additional arrangements that do not violate the provisions of this regulation.

The contract requirement that we are proposing would permit covered entities to exercise control over their business partners' activities and provide documentation of the relationship between the parties, particularly the scope of the uses and disclosures of protected health information that business partners could make. The presence of a contract also would formalize the relationship, better ensuring that key questions such as security, scope of use and disclosure, and access by individuals are adequately addressed and that the roles of the respective parties are clarified. Finally, a contract can bind the business partner to return any protected health information from the covered entity when the relationship is terminated.

In lieu of a contracting requirement, we considered imposing only affirmative duties on covered entities to ensure that their relationships with business partners conformed to the standards discussed in the previous paragraph. Such an approach could be considered less burdensome and restrictive, because we would be leaving it to the parties to determine how to make the standards effective. We rejected this approach primarily because we believe that in the vast majority of cases, the only way that the parties could establish a relationship with these terms would be through contract. We also determined that the value of making the terms explicit through a written contract would better enable the parties to know their roles and responsibilities, as well as better enable the Secretary to exercise her oversight role. In addition, we understand that most covered entities already enter into contracts in these situations and therefore this proposal would not disturb general business practice. We invite comment on whether there are other contractual or non-contractual approaches that would afford an adequate level of protection to individuals' protected health information. We also invite comment on the specific provisions and terms of the proposed approach.

We are proposing one exception to the contracting requirement: when a covered entity consults with or makes a referral to another covered entity for the treatment of an individual, we would propose that the sharing of protected health information pursuant to that consultation or referral not be subject to the contracting requirement described above. See proposed § 164.506(e)(1)(i). Unlike most business partner relationships, which involve the systematic sharing of protected health information under a business relationship, consultation and referrals for treatment occur on a more informal basis among peers, and are specific to a particular individual. Such exchanges of information for treatment also appear to be less likely to raise concerns about further impermissible use or disclosure, because health care providers receiving such information are unlikely to have a commercial or other interest in using or disclosing the information. We invite comment on the appropriateness of this exception, and whether there are additional exceptions that should be included in the final regulation.

We note that covered health care providers receiving protected health information for consultation or referral purposes would still be subject to this rule, and could not use or disclose such protected health information for a purpose other than the purpose for which it was received (i.e., the consultation or referral). Further, we note that providers making disclosures for consultations or referrals should be careful to inform the receiving provider of any special limitations or conditions to which the disclosing provider has agreed to impose (e.g., the disclosing provider has provided notice to its patients that it will not make disclosures for research).

Under the system that we are proposing, business partners (including business partners that are covered entities) that have contracts with more than one covered entity would have no authority to combine, aggregate or otherwise use for a single purpose protected health information obtained from more than one covered entity unless doing so would have been a lawful use or disclosure for each of the covered entities that supplied the protected health information that is being combined, aggregated or used. In addition, the business partner must be authorized through the contract or arrangement with each covered entity that supplied the protected health information to combine or aggregate the information. For example, a business partner of a health plan would be permitted to disclose information to another health plan for coordination of benefits purposes, if such a disclosure were authorized by the business partner's contract with the covered entity that provided the protected health information. However, a business partner that is performing an audit of a group medical practice on behalf of several health plans could not combine protected health information that it had received from each of the plans, even if the business partner's contracts with the plans attempted to allow such activity, because the plans themselves would not be permitted to exchange protected health information for such a purpose. A covered entity would not be permitted to obtain protected health information through a business partner that it could not otherwise obtain itself.

We further note that, as discussed above in section II.C.4, under our proposal a business partner generally could create a database of de-identified health information drawn from the protected health information of more than one covered entity with which it does business, and could use and disclose information and analyses from the database as they see fit, as long as there was no attempt to re-identify the data to create protected health information. In the example from the preceding paragraph, the business partner could review the utilization patterns of a group medical practice on behalf of several groups of plans by establishing a data base of de-identified health information drawn from all of its contracts with covered entities and review the use patterns of all of the individuals in the data base who had been treated by the medical group. The results of the analyses could be used by or distributed to any person, subject to the limitation that the data could not be identified. We would caution that business partners releasing such information and analyses would need to ensure that they do not inadvertently disclose protected health information by releasing examples or discussing specific cases in such a way that the information could be identified by people receiving the analysis or report.

c. *Accountability.* We are proposing that covered entities be accountable for the uses and disclosures of protected health information by their business partners. A covered entity would be in violation of this rule if the covered entity knew or reasonably should have known of a material breach of the contract by a business partner and it failed to take reasonable steps to cure the breach or terminate the contract. See proposed § 164.506(e)(2)(iii). A covered entity that is aware of impermissible uses and disclosures by a business partner would be responsible for taking such steps as are necessary to prevent further improper use or disclosures and, to the extent practicable, for mitigating any harm caused by such violations.

This could include, for example, requiring the business partner to retrieve inappropriately disclosed information (even if the business partner must pay for it) as a condition of continuing to do business with the covered entity. A covered entity that knows or should know of impermissible use of protected health information by its business partner and fails to take reasonable steps to end the breach would be in violation of this rule.

Where a covered entity acts as a business partner to another covered entity, the covered entity that is acting as business partner would also be responsible for any violations of the regulation.

We considered requiring covered entities to terminate relationships with business partners if the business partner committed a serious breach of contact terms required by this subsection or if the business partner exhibited a pattern or practice of behavior that resulted in repeated breaches of such terms. We rejected that approach because of the substantial disruptions in business relationships and customer service when terminations occur. We instead require the covered entity to take reasonable steps to end the breach and mitigate its effects. We would expect covered entities to terminate the arrangement if it becomes clear that a business partner cannot be relied upon to maintain the privacy of protected health information provided to it. We invite comments on our approach here and whether requiring automatic termination of business partner contracts would be warranted in any circumstances.

We also considered imposing more strict liability on covered entities for the actions of their business partners, just as principals are strictly liable for the actions of their agents under common law. We decided, however, that this could impose too great a burden on covered entities, particularly small providers. We are aware that, in some cases, the business partner will be larger and more sophisticated with respect to information handling than the covered entity. Therefore we instead opted to propose that covered entities monitor use of protected health information by business partners, and be held responsible only when they knew or reasonably should have known of improper use of protected health information.

Our intention in this subsection is to recognize the myriad business relationships that currently exist and to ensure that when they involve the exchange of protected health information, the roles and responsibilities of the different parties with respect to the protected health information are clear. We do not propose to fundamentally alter the types of business relationships that exist in the health care industry or the manner in which they function. We request comments on the extent to which our proposal would disturb existing contractual or other arrangements among covered entities and business partners.

6. Application to Information About Deceased Persons (§ 164.506(f))

[Please label comments about this section with the subject: ''Deceased persons'']

We are proposing that information otherwise protected by these regulations retain that protection for two years after the death of the subject of the information. The only exception that we are proposing is for uses and disclosures for research purposes.

HIPAA includes no temporal limitations on the application of the privacy protections. Although we have the authority to protect individually identifiable health information maintained by a covered entity indefinitely, we are proposing that the requirements of this rule generally apply for only a limited period, as discussed below. In traditional privacy law, privacy interests, in the sense of the right to control use or disclosure of information about oneself, cease at death. However, good arguments exist in favor both of protecting and not protecting information about the deceased. Considering that one of the underlying purposes of health information confidentiality is to encourage a person seeking treatment to be frank in the interest of obtaining care, there is good reason for protecting information even after death. Federal agencies and others sometimes withhold sensitive information, such as health information, to protect the privacy of surviving family members. At the same time, perpetual confidentiality has serious drawbacks. If information is needed for legitimate purposes, the consent of a living person legally authorized to grant such consent must be obtained, and the further from the date of death, the more difficult it may be to identify the person. The administrative burden of perpetual protection may eventually outweigh the privacy interests served.

The proposed two-year period of confidentiality, with an exception for uses and disclosures for research purposes, would preserve dignity and respect by preventing uncontrolled disclosure of information immediately after death while allowing access to the information for proper purposes during this period and for any purpose thereafter. We would not subject the use or disclosure of protected health information of deceased individuals to the requirements in proposed § 164.510(j) governing most uses and disclosures for research because we believe that it is important to remain as consistent as possible with the Common Rule. The Common Rule does not consider deceased persons to be ''human subjects'' and therefore they have never been covered in the standard research protocol assessments conducted under the Common Rule. The Department of Health and Human Services will examine this issue in the context of an overall assessment of the Common Rule. Pending the outcome of this examination, we concluded that this exception was warranted so as not to interfere with standard research practice. We invite comments on whether the exception that we are proposing is necessary, or whether existing research using the protected health information of deceased individuals could proceed under the requirements of proposed § 164.510(j).

Under our proposal, and subject to the exceptions discussed above, the right to control the individual's health information within that two-year time period would be held by an executor or administrator, or in the absence of such an officer, by next-of-kin, as determined under applicable law, or in absence of both, by the holder of the health information. This is reflected in the proposed definition of ''individual'' discussed above. The legally authorized representative would make decisions for the individual with regard to uses or disclosures of the information for purposes not related to treatment, payment or health care operations. Likewise, an authorized representative could exercise the individual rights of inspection, copying, amendment or correction under proposed §§ 164.514 and 164.516.

Under our proposal, information holders could choose to keep information confidential for a longer period. These proposed rules also would not override any legally required prohibitions on disclosure for longer periods.

One area of concern regarding the proposed two-year period of protection relates to information on individual genetic make-up or individual diseases and conditions that may be hereditary. Under the proposed rules, covered entities would be legally allowed to use such information or to disclose records to others, such as commercial collectors of information, two years after the death of the individual. Since genetic information about one family member may reveal health information about other members of that family, the health data confidentiality of living relatives could be compromised by such uses or disclosures. Likewise, information regarding the hereditary diseases or conditions of the deceased person may reveal health information about living relatives. In the past, information that may not have been legally protected was *de facto* protected for most people because of the difficulty of its collection and aggregation. With the dramatic proliferation of large electronic databases of information about individuals, growing software-based intelligence, and the declining cost of linking information from disparate sources, such information could now be more readily and cost-effectively accessed.

While various State laws have been passed specifically addressing privacy of genetic information, there is currently no federal legislation that deals with these issues. We considered extending the two-year period for genetic and hereditary information, but were unable to construct criteria for protecting the possible privacy interests of living children without creating extensive burden for information holders and hampering health research. We invite comments on whether further action is needed in this area and what types of practical provisions may be appropriate to protect genetic and hereditary health information.

7. Adherence to the Notice of Information Practices (§ 164.506(g))

[Please label comments about this section with the subject: ''Adherence to notice'']

In § 164.506(g), we are proposing that covered plans and providers be required to adhere to the statements reflected in the notice of information practices that would be required under proposed § 164.512. In binding covered plans and providers to their notices, we intend to create a system where open and accurate communication between entities and individuals would become necessary and routine. The corollary to this general rule is that the covered plan or provider would be permitted to modify its notice at any time.

The information practices reflected in the most recent notice would apply to all protected health information regardless of when the information was collected. For example, if information was collected during a period when the notice stated that no disclosures would be made to researchers, and the covered plan or provider later decided that it wanted to disclose information to researchers, the entity would then need to revise its notice. The entity would be permitted to disclose all of the information in its custody to researchers as long as the notice is revised and re-distributed as provided below in § 164.512. We considered permitting a covered entity to change its information practices only with respect to protected health information obtained after it revised its notice. Such a requirement would ensure individuals that the notice they received when they disclosed information to the covered entity would continue to apply to that information. We rejected that approach because compliance with such a standard would require covered entities to segregate or otherwise mark information to be based on the information practices that were in effect at different times. Such an approach would make covered entities extremely reluctant to revise the information practices, and otherwise would be extremely burdensome to administer.

We are concerned that by requiring covered plans and providers to adhere to the practices reflected in their notice, we would encourage entities to create broad, general notices so that all possible uses, disclosures and other practices would be included. Such broad notices would not achieve the goals of open and accurate communication between entities and individuals. We welcome comments on this requirement and alternative proposals to achieve the same goals.

8. Application to Covered Entities That Are Components of Organizations That Are Not Covered Entities

[Please label comments about this section with the subject: ''Component entities'']

In this section we describe how the provisions of this proposed rule apply to persons or organizations that provide health care or have created health plans but are primarily engaged in other unrelated activities. Examples of such organizations include schools that operate on-site clinics, employers who operate self-funded health plans, and information processing companies that include a health care services component. The health care component (whether or not separately incorporated) of the organization would be the covered entity. Therefore, any movement of protected health information into another component of the organization would be a ''disclosure,'' and would be lawful only if such disclosure would be authorized by this regulation. In addition, we propose to require such entities to create barriers to prevent protected health information from being used or disclosed for other activities not authorized or permitted under these proposed rules.

For example, schools frequently employ school nurses or operate on-site clinics. In doing so, the nurse or clinic component of the school would be acting as a provider, and must conform to this proposed rule. School clinics would be able to use protected health information obtained in an on-site clinic for treatment and payment purposes, but could not disclose it to the school for disciplinary purposes except as permitted by this rule. Similarly, an employee assistance program of an employer could meet the definition of ''provider,'' particularly if health care services are offered directly by the program. Protected health information obtained by the employee assistance program could be used for treatment and payment purposes, but not for other purposes such as hiring and firing, placement and promotions, except as may be permitted by this rule.

D. Uses and Disclosures With Individual Authorization (§ 164.508)

[Please label comments about this section With the subject: ''Individual authorization'']

This section addresses the requirements that we are proposing when protected health information is disclosed pursuant to the individual's explicit authorization. The regulation would require that covered entities have authorization from individuals before using or disclosing their protected health information for any purpose not otherwise recognized by this regulation. Circumstances where an individual's protected health information may be used or disclosed without authorization are discussed in connection with proposed §§ 164.510 and 164.522 below.

This section proposes different conditions governing such authorizations in two situations in which individuals commonly authorize covered entities to disclose information:

- Where the individual initiates the authorization because he or she wants a covered entity to disclose his or her record, and
- Where a covered entity asks an individual to authorize it to disclose or use information for purposes other than treatment, payment or health care operations.

In addition, this section proposes conditions where a covered entity or the individual initiates an authorization for use or disclosure of psychotherapy notes or research information unrelated to treatment. See discussion above in section II.C.1.c.

Individually identifiable health information is used for a vast array of purposes not directly related to providing or paying for an individual's health care. Examples of such uses include targeted marketing of new products and assessing the eligibility of an individual for certain public benefits or for commercial products based on their health status. Under these rules, these types of uses and disclosures could only be made by a covered entity with the specific authorization of the subject of the information. The requirements proposed in this section are not intended to interfere with normal uses and disclosures of information in the health care delivery or payment process, but only to permit control of uses extraneous to health care. The restrictions on disclosure that the regulation would apply to covered entities may mean that some existing uses and disclosures of information could take place only if the individual explicitly authorized them under this section.

Authorization would be required for these uses and disclosures because individuals probably do not envision that the information they provide when getting health care would be disclosed for such unrelated purposes. Further, once a patient's protected health information is disclosed outside of the treatment and payment arena, it could be very difficult for the individual to determine what additional entities have seen, used and further disclosed the information. Requiring an authorization from the patient for such uses and disclosures would enhance individuals' control over their protected health information.

We considered requiring a uniform set of requirements for all authorizations, but concluded that it would be appropriate to treat authorizations initiated by the individual differently from authorizations sought by covered entities. There are fundamental differences in the uses of information and in the relationships and understandings among the parties in these two situations. When individuals initiate authorizations, they are more likely to understand the purpose of the release and to benefit themselves from the use or disclosure. When a covered entity asks the individual to authorize disclosure, we believe the entity should make clear what the information will be used for, what the individual's rights are, and how the covered entity would benefit from the requested disclosure.

Individuals seek disclosure of their health information to others in many circumstances, such as when applying for life or disability insurance, when government agencies conduct suitability investigations, and in seeking certain job assignments where health is relevant. Another common instance is tort litigation, where an individual's attorney needs individually identifiable health information to evaluate an injury claim and asks the individual to authorize disclosure of records relating to the injury to the attorney.

There could also be circumstances where the covered entity asks an individual to authorize use or disclosure of information, for example to disclose it to a subsidiary to market life insurance to the individual. Similarly, the covered entity might ask that the individual authorize it to send information to a person outside that covered entity—possibly another covered entity or class of covered entity—for purposes outside of treatment, payment, or health care operations. See proposed § 164.508(a)(2)(ii).

1. Requirements When the Individual Has Initiated the Authorization

We are proposing several requirements that would have to be met in the authorization process when the individual has initiated the authorization.

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

We are proposing no limitations on the information to be disclosed. If an individual wishes to authorize a covered entity to disclose his or her entire medical record, the authorization could so specify. But in order for the covered entity to disclose the entire medical record, the authorization would have be specific enough to ensure that individuals have a clear understanding of what information is to be disclosed under the circumstances. For example, if the Social Security Administration seeks authorization for release of all health information to facilitate the processing of benefit applications, then the description would need to specify ''all health information.''

We would note that our proposal does not require a covered entity to disclose information pursuant to an individual's authorization. Therefore individuals may face reluctance on the part of covered entities that receive authorizations requiring them to classify and selectively disclose information when they do not benefit from the activity. Individuals would need to consider this when specifying the information in the authorization. Covered entities may respond to requests to analyze and separate information for selective disclosure by providing the entire record to the individual, who may then redact and release the information to others.

We do not propose to require an authorization initiated by an individual to state a purpose. When the individual has initiated the authorization, the entity would not need to know why he or she wants the information disclosed. Ideally, anyone asking an individual to authorize release of individually identifiable health information would indicate the purpose and the intended uses. We are unable to impose requirements on the many entities that make such requests, and it would not be feasible to ask covered entities to make judgments about intended uses of records that are disclosed. In the absence of legal controls in this situation, the prudent individual would obtain a clear understanding of why the requester needs the information and how it would be used.

We are proposing that the authorization would be required to identify sufficiently the covered entity or covered entities that would be authorized to use or disclose the protected health information by the authorization. Additionally, the authorization would be required to identify the person or persons that would be authorized to use or receive the protected health information with sufficient specificity to reasonably permit a covered entity responding to the authorization to identify the authorized user or recipient. When an authorization permits a class of covered entities to disclose information to an authorized person, each covered entity would need to know with reasonable certainty that the individual intended for it to release protected health information under the authorization.

Often, individuals provide authorizations to third parties, who present them to one or more covered entities. For example, an authorization could be completed by an individual and provided to a government agency, authorizing the agency to receive medical information from any health care provider that has treated the individual within a defined period. Such an authorization would be permissible (subject to the other requirements of this part) if it sufficiently identifies the government entity as the recipient of the disclosures and it sufficiently identifies the health care providers who would be authorized to release the individual's protected health information under the authorization.

We are proposing that the authorization must state a specific expiration date. We considered providing an alternative way of describing the termination of the authorization, such as ''the conclusion of the clinical trial,'' or ''upon acceptance or denial of this application for life insurance'' (an ''event''), but we are concerned that covered entities could have difficulty implementing such an approach. We also considered proposing that if an expiration date were indicated on the authorization, it be no more than two or three years after the date of the signature. We are soliciting comment on whether an event can be a termination specification, and whether this proposed rule should permit covered entities to honor authorizations with ''unlimited'' or extremely lengthy expiration dates or limit it to a set term of years, such as two or three years.

We are proposing that the authorization include a signature or other authentication (e.g., electronic signature) and the date of the signature. If the authorization is signed by an individual other than the subject of the information to be disclosed, that individual would have to indicate his or her authority or relationship with the subject.

The authorization would also be required to include a statement that the individual understands that he or she may revoke an authorization except to the extent that action has been taken in reliance on the authorization.

When an individual authorizes disclosure of health information to other than a covered entity, the information would no longer be protected under this regulation once it leaves the covered entity. Therefore, we propose that the authorization must clearly state that the individual understands that when the information is disclosed to anyone except a covered entity, it would no longer be protected under this regulation.

We understand that the requirements that we are imposing here would make it quite unlikely that an individual could actually initiate a completed authorization, because few individuals would know to include all of these elements in a request for information. We understand that in most instances, individuals accomplish authorizations for release of health records by completing a form provided by another party, either the ultimate recipient of the records (who may have a form authorizing them to request the records from the record holders) or a health care provider or health plan holding the records (who may have a form that documents a request for the release of records to a third party). For this reason, we do not believe that our proposal would create substantial new burdens on individuals or covered entities in cases when an individual is initiating an authorized release of information. We invite comment on whether we are placing new burdens on individuals or covered entities. We also invite comment on whether the approach that we have proposed provides sufficient protection to individuals who seek to have their protected health information used or disclosed.

2. Requirements When the Covered Entity Initiates the Authorization

We are proposing that when covered entities initiate the authorization by asking individuals to authorize disclosure, the authorization be required to include all of the items required above as well as several additional items. We are proposing additional requirements when covered entities initiate the request for authorization because in many cases it could be the covered entity, and not the individual, that achieves the primary benefit of the disclosure. We considered permitting covered entities to request authorizations with only the basic features proposed for authorizations initiated by the individual, for the sake of simplicity and consistency. However, we believe that additional protections would be merited when the entity that provides or pays for health care requests an authorizations to avert possible coercion.

When a covered entity asks an individual to sign an authorization, we propose to require that it provide on the authorization a statement that identifies the purposes for which the information is sought as well as the proposed uses and disclosures of that information. The required statements of purpose would provide individuals with the facts they need to make an informed decision as to whether to allow release of the information. Covered entities and their business partners would be bound by the statements provided on the authorization, and use or disclosure by the covered entity inconsistent with the statement would constitute a violation of this regulation. We recognize that the covered entities cannot know or control uses and disclosures that will be made by persons who are not business partners to whom the information is properly disclosed. As discussed above, authorizations would need to notify individuals that when the information is disclosed to anyone except a covered entity, it would no longer be protected under this regulation.

We propose to require that authorizations requested by covered entities be narrowly tailored to authorize use or disclosure of only the protected health information necessary to accomplish the purpose specified in the authorization. The request would be subject to the minimum necessary requirement as discussed in section II.C.2. We would prohibit the use of broad or blanket authorizations requesting the use or disclosure of protected health information for a wide range of purposes. Both the information that would be used or disclosed and the specific purposes for such uses or disclosures would need to be specified in the notice.

We are proposing that when covered entities ask individuals to authorize use or disclosure for purposes other than for treatment, payment, or health care operations, they be required to advise individuals that they may inspect or copy the information to be used or disclosed as provided in proposed § 164.514, that they may refuse to sign the authorization, and that treatment and payment could not be conditioned on the patient's authorization. For example, a request for authorization to use or disclose protected health information for marketing purposes would need to clearly state that the individual's decision would have no influence on his or her health care treatment or payment. In addition, we are proposing that when a covered entity requests an authorization, it must provide the individual with a copy of the signed authorization form.

Finally, we are proposing that when the covered entity initiates the authorization and the covered entity would be receiving financial or in-kind compensation in exchange for using or disclosing the health information, the authorization would include a statement that the disclosure would result in commercial gain to the covered entity. For example, a health plan may wish to sell or rent its enrollee mailing list. A pharmaceutical company may offer a provider a discount on its products if the provider can obtain authorization to disclose the demographic information of patients with certain diagnoses so that the company can market new drugs to them directly. A pharmaceutical company could pay a pharmacy to send marketing information to individuals on its behalf. Each such case would require a statement that the requesting entity will gain financially from the disclosure.

We considered requiring a contract between the provider and the pharmaceutical company in this type of arrangement, because such a contract could enhance protections and enforcement options against entities who violate these rules. A contract also would provide covered entities a basis to enforce any limits on further use or disclosures by authorized recipients. Although we are not proposing this approach now, we are soliciting comment on how best to protect the interests of the patient when the authorization for use or disclosure would result in commercial gain to the covered entity.

3. Model Forms

Covered entities and third parties that wish to have information disclosed to them would need to prepare forms for individuals to use to authorize use or disclosure. A model authorization form is displayed in Appendix to this proposed rule. We considered presenting separate model forms for the two different types of authorizations (initiated by the individual and not initiated by the individual). However, this approach could be subject to misuse and be confusing to covered entities and individuals, who may be unclear as to which form is appropriate in specific situations. The model in the appendix accordingly is a unitary model, which includes all of the requirements for both types of authorization.

4. Plain Language Requirement

We are proposing that all authorizations must be written in plain language. If individuals cannot understand the authorization they may not understand the results of signing the authorization or their right to refuse to sign. See section II.F.1 for more discussion of the plain language requirement.

5. Prohibition on Conditioning Treatment or Payment

We propose that covered entities be prohibited, except in the case of clinical trial as described below, from conditioning treatment or payment for health care on obtaining an authorization for purposes other than treatment, payment or health care operations. This is intended to prevent covered plans and providers from coercing individuals into signing an authorization for a disclosure that is not necessary for treatment, payment or health care operations. For example, a provider could not refuse to treat an individual because the individual refused to authorize a disclosure to a pharmaceutical manufacturer for the purpose of marketing a new product.

We propose one exception to this provision: health care providers would be permitted to condition treatment provided as part of a clinical trial on obtaining an authorization from the individual that his or her protected health information could be used or disclosed for research associated with such clinical trial. Permitting use of protected health information is part of the decision to receive care through a clinical trial, and health care providers conducting such trials should be able to condition participation in the trial on the individual's willingness to authorize that his or her protected health information be used or disclosed for research associated with the trial. We note that the uses and disclosures would be subject to the requirements of § 164.510(j) below.

Under the proposal, a covered entity would not be permitted to obtain an authorization for use or disclosure of information for treatment, payment or health care operations unless required by applicable law. Where such an authorization is required by law, however, it could not be combined in the same document with an individual authorization to use or disclosure of protected health information for any purpose other than treatment, payment or health care operations (e.g., research). We would require that a separate document be used to obtain any other individual authorizations to make it clear to the individual that providing an authorization for such other purpose is not a condition of receiving treatment or payment.

6. Inclusion in the Accounting and Disclosures

As discussed in section II.H.6, we propose that covered entities be required to keep a record of all disclosures for purposes other than treatment, payment or health care operations, including those made pursuant to authorization. In addition, we propose that when an individual requests such an accounting or requests a copy of a signed authorization form, the covered entity must give a copy to the individual. See proposed § 164.515.

7. Revocation of an Authorization by the Individual

We are proposing that an individual be permitted to revoke an authorization at any time except to the extent that action has been taken in reliance on the authorization. See proposed § 164.508(e). That is, an individual could change her or his mind about an authorization and cancel it, except that she or he could not thereby prevent the use or disclosure of information if the recipient has already acted in reliance on the authorization. For example, an individual might cancel her or his authorization to receive future advertisements, but the entity may be unable to prevent mailing of the advertisements that the covered entity or third party has already prepared but not yet mailed.

An individual would revoke the old authorization and sign a new authorization when she or he wishes to change any of the information in the original authorization. Upon receipt of the revocation, the covered entity would need to stop processing the information for use or disclosure to the greatest extent practicable.

8. Expired, Deficient, or False Authorization

The model authorization form or a document that includes the elements set out at proposed § 164.508 would meet the requirements of this proposed rule and would have to be accepted by the covered entity. Under § 164.508(b), there would be no ''authorization'' within the meaning of the rules proposed below if the submitted document has any of the following defects:

- The date has expired;
- On its face it substantially fails to conform to any of the requirements set out in proposed § 164.508, because it lacks an element;
- It has not been filled out completely. Covered entities may not rely on a blank or incomplete authorization;
- The authorization is known to have been revoked; or
- The information on the form is known by the person holding the records to be materially false.

We understand that it would be difficult for a covered entity to confirm the identity of the person who signed the authorization. We invite comment on reasonable steps that a covered entity could take to be assured that the individual who requests the disclosure is whom she or he purports to be.

E. Uses and Disclosures Permitted Without Individual Authorization (§ 164.510)

[Please label comments about this section with the subject: ''Introduction to uses and disclosures without individual authorization'']

This section describes uses and disclosures of protected health information that covered entities could make for purposes other than treatment, payment, and health care operations without individual authorization, and the conditions under which such uses and disclosures could be made. We propose to allow covered entities to use or disclose protected health information without individual authorization for such purposes if the use or disclosure would comply with the applicable requirements of this section.

These categories of allowable uses and disclosures are designed to permit and promote key national health care priorities, and to ensure that the health care system operates smoothly. For each of these categories, this rule would permit—but not require—the covered entity to use or disclose protected health information without the individual's authorization. Some covered entities could conclude that the records they hold, or portions of them, should not be used or disclosed for one or more of these permitted purposes without individuals' authorization (absent a law mandating such disclosure), even under the conditions imposed here. The proposed regulation is intended to reflect the importance of safeguarding individuals' confidentiality, while also enabling important national priority activities that require protected health information.

We considered permitting uses and disclosures only where law affirmatively requires the covered entity to use or disclose protected health information. However, because the activities described below are so important to the population as a whole, we decided to permit a covered entity to use or disclose information to promote those activities even when such activities are not legally mandated. In some cases, however, we would permit a use or disclosure only when such use or disclosure is authorized by other law. The requirements for verification of legal authority are discussed in each relevant section.

Where another law forbids the use or disclosure of protected health information without the individual's authorization, nothing in this section would permit such use or disclosure.

Other law may require use or disclosure of protected health information. If such a use or disclosure is not otherwise addressed in proposed § 164.510(b) through (m), we would in proposed § 164.510(n) permit covered entities to use or disclose protected health information without individual authorization pursuant to any law that mandates such use or disclosure. To be in compliance with this rule, the covered entity must meet the requirements of such other law requiring the use or disclosure. Similarly, nothing in this rule would provide authority for a covered entity to restrict or refuse to make a use or disclosure mandated by other law.

The HIPAA legislative authority generally does not bring the entities that receive disclosures pursuant to this section, including public health authorities, oversight and law enforcement agencies, researchers, and attorneys, under the jurisdiction of this proposed rule. We therefore generally cannot propose restrictions on the further use and disclosure of protected health information obtained by the recipients of these disclosures (unless the recipient is also a covered entity). We believe, however, that in most instances it is sound policy to restrict further uses and disclosures of such protected health information. For example, the Secretary's Recommendations proposed that protected health information obtained by researchers not be further disclosed except for emergency circumstances, for a research project that meets certain conditions, and for oversight of research. We believe that federal legislation should include appropriate restrictions on further use and disclosure of protected health information received by entities for purposes such as those described in this section. We note that, under S.578 (introduced by Senator Jeffords), protected health information disclosed for oversight could not be used against the subject of the protected health information unless the action arises out of and is directly related to a health care fraud or a fraudulent claim for benefits, unless such use is judicially authorized. We believe such safeguards strike the right balance between encouraging national priority oversight activities and protecting individuals' privacy.

The provisions of this section contain requirements related to use and requirements related to disclosure, as appropriate to each of the purposes discussed. For many of these purposes, only requirements relating to disclosure are proposed because there are no appropriate internal uses for such a purpose. Examples include disclosures for next-of-kin and disclosures for banking and financial purposes.

For many of these permitted disclosures, we would require the covered entity to verify the identity of the requestor and his or her legal authority to make the request. Requirements for verifying the identity and authority of requests for information are further discussed in II.G, ''Administrative Requirements.'' As discussed in more detail in section II.G.3. of this preamble, the verification requirement would apply where the identity of the person making the request is not already known to the covered entity (e.g., where the disclosure is not part of a routine business transaction). We would ask health plans and health care providers to take reasonable steps to verify the identity of persons requesting protected health information, such as asking to see a badge or other proof of the identity of government officials, and would allow covered entities to rely on the statement of government officials and others regarding the legal authority for the activity. We would not require covered entities to make an independent inquiry into the legal authority behind requests for protected health information.

The provisions below would permit covered entities to use or disclose protected health information without individual authorization, pursuant to certain requirements. Although health care clearinghouses would be defined as covered entities under this rule, in most instances clearinghouses will be receiving and maintaining protected health information as the business partner of a covered health plan or provider. In such cases, proposed § 164.510(a)(2) provides that the clearinghouses that hold protected health information as business partners would not be permitted to make uses or disclosures otherwise permitted by this section unless such uses or disclosures also were permitted under the terms of the contract between the clearinghouse and the business partner.

1. Uses and Disclosures for Public Health Activities (§ 164.510(b))

[Please label comments about this section with the subject: ''Public health'']

We propose to permit covered entities to disclose protected health information without individual authorization to public health authorities carrying out public health activities authorized by law, to non-governmental entities authorized by law to carry out public health activities, and to persons who may be at risk of contracting or spreading a disease (when other law authorizes notification). Where the covered entity also is a public health agency, such as a public hospital or local health department, it would be permitted to use protected health information in all cases in which it would be permitted to disclose such information for public health activities under this section.

a. *Importance of public health and need for protected health information.* Public health authorities are responsible for promoting health and quality of life by preventing and controlling disease, injury, and disability. Inherent in the collection of information for public health activities is a balancing of individual versus communal interests. While the individual has an interest in maintaining the privacy of his or her health information, public health authorities have an interest in the overall health and well-being of the entire population of their jurisdictions. To accomplish this, public health authorities engage in a number of activities, including: traditional public health surveillance; investigations and interventions with respect to communicable diseases; registries (such as immunization or cancer registries); programs to combat diseases that involve contacting infected persons and providing treatment; and actions to prevent transmission of serious communicable diseases.

Public health activities also include regulatory investigations and interventions such as pre-market review of medical products, and evaluations of the risk-benefit profile of a drug or medical product before and after approval (relying on critical epidemiological techniques and resources such as HMO claims databases and medical records). Public health agencies use the results of analyses to make important labeling changes and take other actions, such as the removal of non-compliant products from the market.

We considered requiring individual authorization for certain public health disclosures, but rejected this approach because many important public health activities would not be possible if individual authorization were required. In the case of contagious diseases, for example, if individual authorization were required before individually identifiable information could be provided to public health workers, many other people who may be harboring contagious diseases may be missed by efforts to halt the spread of disease because they failed to provide the appropriate individual authorization. Their failure to authorize could place the general population at risk for contracting an infectious disease. Furthermore, always requiring individual authorization to disclose protected health information to public health authorities would be impractical due to the number of reports and the variety of sources from which they are made. If individuals were permitted to opt out from having their information included in these public health systems, the number of persons with a particular condition would be undercounted. Furthermore, the persons who did authorize the inclusion of their information in the system might not be representative of all persons with the disease or condition.

We also considered limiting certain public health disclosures to de-identified health information. However, identifiable information could be required in order to track trends in a disease over time, and to assess the safety of medical treatments. While de-identified information could be appropriate for many public health activities, there are also many public health activities that require individual identifiers. We decided not to attempt to define specific public health activities for which only de-identified information could be disclosed, in part because public health data collection requirements would be better addressed in public health laws, and in part to reflect the variation in information technologies available to public health authorities. Instead, we rely on the judgment of public health authorities as to what information would be necessary for a public health activity. See discussion in section II.C.2.

b. *Public health activities.* We intend a broad reading of the term ''public health activities'' to include the prevention or control of disease, injury, or disability. We considered whether to propose a narrow or broad scope of public health activities for which disclosure without individual authorization would be permitted. For the reasons described above, we believe that both the general public and individual interests are best served by a broad approach to public health disclosures.

We therefore propose that covered entities be permitted to disclose protected health information to public health authorities for the full range of public health activities described above, including reporting of diseases, injuries, and conditions, reporting of vital events such as birth and death to vital statistics agencies, and a variety of activities broadly covered by the terms public health surveillance, public health investigation, and public health intervention. These would include public health activities undertaken by the FDA to evaluate and monitor the safety of food, drugs, medical devices, and other products. These terms would be intended to cover the spectrum of public health activities carried out by federal, State, and local public health authorities. The actual authorities and terminology used for public health activities will vary under different jurisdictions. We do not intend to disturb or limit current public health activities.

c. *Permitted recipients of disclosures for public health activities.* Disclosures without individual authorization for public health activities would be permitted to be made to only three types of persons: public health authorities, non-governmental entities authorized by law to carry out public health activities, and persons who may be at risk of contracting or spreading a disease, if other law authorizes notification.

i. *Public health authorities.*

We propose to define ''public health authority'' broadly, based on the function being carried out, not the title of the public entity. Therefore, disclosures under this proposed rule would not be limited to traditional public health entities such as State health departments. Other government agencies and entities carry out public health activities in the course of their missions. For example, the Occupational Safety and Health Administration, the Mine Safety and Health Administration, and the National Institute for Occupational Safety and Health conduct public health investigations related to occupational health and safety. The National Transportation Safety Board investigates airplane and train crashes in an effort to reduce mortality and injury by making recommendations for safety improvements. Similar inquiries are conducted by the military services. The Food and Drug Administration reviews product performance prior to marketing, and investigates adverse events reported after marketing by industries, health professionals, consumers, and others. The Environmental Protection Agency investigates the effects of environmental factors on health. The definition of public health authority reflects the need for access to data and information including protected health information by these other agencies and authorities consistent with their official mandates under applicable law.

ii. *Non-governmental entities carrying out public health activities.*

The proposed rule would further provide that disclosures may be made not only to government agencies, but also to other public and private entities as otherwise required or authorized by law. For example, this would include tracking medical devices, where the initial disclosure is not to a government agency, but to a device manufacturer that collects information under explicit legal authority, or at the direction of the Food and Drug Administration. Also, the cancer registries mentioned above could be operated by non-profit organizations such as universities funded by public health authorities which receive reports from physicians and laboratories pursuant to State statutory requirements to report.

We considered limiting public health disclosures to only government entities, but the reality of current public health practice is that a variety of activities are conducted by public health authorities in collaboration with non-governmental entities. Federal agencies also use a variety of mechanisms including contracts, grants, cooperative agreements, and other agreements such as memoranda of understanding to carry out and support public health activities. These relationships could be based on specific or general legal authorities. It is not our intent to disturb these relationships. Limiting the ability to collaborate with other entities and designate them to receive protected health information, could potentially have an adverse impact on public health practice.

iii. *Persons who may be at risk of contracting or spreading a disease.*

The proposed rule would allow disclosure to a person who could have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition and is authorized by law to be notified as necessary in the conduct of a public health intervention or investigation. Physicians, in carrying out public health interventions authorized by law, can notify persons who have been exposed to a communicable disease, or who otherwise may be at risk of contracting or spreading a disease or condition. That notification may implicitly or explicitly reveal the identity of the individual with the disease to which the person could have been exposed, but should be permitted as a disclosure in the course of a legally authorized public health intervention or investigation. The proposed rule would not (and, under the HIPAA legislative authority, cannot) impose a confidentiality obligation on the person notified.

d. *Additional requirements.* Under proposed § 164.518(c), covered entities would have to verify the identity of the person requesting protected health information and the legal authority supporting that request, before the disclosure would be permitted under this subsection. Preamble section II.G.3 describes these requirements in more detail.

We note that to the extent that the public health authority is providing treatment as defined in proposed § 164.504, the public health authority would be a covered health care provider for purposes of that treatment, and would be required to comply with this regulation.

We also note that the preemption provision of the HIPAA statute creates a special rule for a subset of public health disclosures: this regulation cannot preempt State law regarding ‘‘public health surveillance, or public health investigation or intervention * * *’’.

2. Use and Disclosure for Health Oversight Activities. (§ 164.510(c))

[*Please label comments about this section with the subject: ‘‘Health oversight*’’]

In section § 164.510(c), we propose to allow covered entities to disclose protected health information to public oversight agencies (and to private entities acting on behalf of such agencies) without individual authorization, for health oversight activities authorized by law. In cases in which a covered entity is also an oversight agency, it would be permitted to use protected health information in all cases in which it would be permitted to disclose such information for health oversight activities under this section.

a. *Importance of oversight and need for protected health information.* Oversight activities are critical to support national priorities, including combating fraud in the health care industry, ensuring nondiscrimination, and improving the quality of care. The goals of public agencies' oversight activities are: to monitor the fiscal and programmatic integrity of health programs and of government benefit programs; to ensure that payments or other benefits of these programs are being provided properly; to safeguard health care quality; to monitor the safety and efficacy of medical products; and to ensure compliance with statutes, regulations, and other administrative requirements applicable to public programs and to health care delivery.

Oversight activities are a national priority in part because of the losses in the healthcare system due to error and abuse. For example, the HHS Office of Inspector General recently estimated losses due to improper Medicare benefit payments to be about seven percent. See ‘‘Improper Fiscal Year 1998 Medicare Fee-For Service-Payments,’’ transmittal from Inspector General June Gibbs Brown to HCFA Administrator Nancy-Ann Min DeParle (February 9, 1999). Similarly, the final report of the President's Advisory Commission on Consumer Protection and Quality in the Health Care Industry concluded that ‘‘employing the extensive knowledge and expertise of organizations that oversee health care quality * * * is essential to quality improvement.’’ (http://www.hcqualitycommission.gov/final/chap09.html)

There are certain oversight activities done as statistical inquiries that can be conducted without direct access to individually identifiable health information. However, many instances exist in which government oversight agencies, and private entities under contracting to act on their behalf, need to examine individually identifiable health information to conduct their investigations effectively. For example, to determine whether a hospital has engaged in fraudulent billing practices, it could be necessary to examine billing records for a set of individual cases. Billing abuses are detected by cross-checking the records of specific patients to see the medical documentation in support of a service. To determine whether a health plan is complying with federal or State health care quality standards, it may be necessary to examine individually identifiable health information. Other inquiries require review of individually identifiable health information to identify specific instances of the anomalies in treatment or billing patterns detected in statistical analysis. Even in most statistical inquiries of the type just described, in a paper environment particular patient charts must be examined, and the patient's name would be disclosed because it would be on each page of the chart.

b. *Proposed requirements.* Specifically, we would permit covered entities to disclose protected health information without individual authorization to a health oversight agency to conduct oversight activities authorized by law. Disclosures also could be made to private entities working under a contract with or grant of authority from one or more of the government oversight agencies described above. As discussed below, oversight activities by private entities operating pursuant to contracts with covered entities, such as accreditation organizations, would not be permitted to receive information under this provision, even if accreditation by such an organization is recognized by law as fulfilling a government requirement or condition of participation in a government program (often referred to as ''deemed status'').

Under our rule, oversight activities would include conducting or supervising the following activities: Audits; investigations; inspections; civil, criminal or administrative proceedings or actions; and other activities necessary for appropriate oversight of the health care system, of government benefit programs for which health information is relevant to beneficiary eligibility, and of government regulatory programs for which health information is necessary for determining compliance with program standards. This regulation does not create any new right of access to health records by oversight agencies, and could not be used as authority to obtain records not otherwise legally available to the oversight agency.

Under our rule, a health oversight agency would be defined as a public agency authorized by law to conduct oversight activities relating to the health care system, a government program for which health information is relevant to determining beneficiary eligibility or a government regulatory program for which health information is necessary for determining compliance with program standards. Examples of agencies in the first category would include State insurance commissions, State health professional licensure agencies, Offices of Inspectors General of federal agencies, the Department of Justice, State Medicaid fraud control units, Defense Criminal Investigative Services, the Pension and Welfare Benefit Administration, the HHS Office for Civil Rights, and the FDA. Examples of agencies in the second category include the Social Security Administration and the Department of Education. Examples of agencies in the third category include the workplace safety programs such as the Occupational Health and Safety Administration and the Environmental Protection Agency. Agencies that conduct both oversight and law enforcement activities would be subject to this provision when conducting oversight activities.

In cases where health oversight agencies are working in tandem with other agencies overseeing public benefit programs to address compliance, fraud, or other integrity issues that could span across programs, the oversight activities of the team would be considered health oversight and disclosure to and among team members would be permitted under the proposed rule to the extent permitted under other law. For example, a fraud investigation could attempt to find a pattern of abuse across related programs, such as Medicaid and the supplemental security income program. Protected health information could be disclosed to the team of oversight agencies and could be shared among such agencies for oversight activities.

Public oversight agencies sometimes contract with private entities to conduct program integrity activities on a public agency's behalf. Such audits or investigations may include, for example, program integrity reviews of fraud and abuse in billing Federal and State health care programs; investigations conducted in response to consumer complaints regarding the quality or accessibility of a particular provider, health plan, or facility; and investigations related to disciplinary action against a health care provider, health plan, or health care facility. Covered entities may disclose protected health information to these agents to the extent such disclosure would be permitted to the public oversight body.

In many cases today, public agencies' contracts with private entities conducting investigations on their behalf require the private oversight organization to implement safeguards to protect individual privacy. HIPAA does not provide statutory authority to regulate the contracts between public oversight entities and their agents. However, we encourage public oversight entities to include privacy safeguards in all such contracts, and believe it would be appropriate for federal legislation to impose such safeguards.

In developing our proposal, we considered but rejected the option of providing an exemption from the general rules for situations in which a covered entity has a contract with a private accreditation organization to conduct an accreditation inspection. In such instances, the accreditation organization is performing a service for the covered entity much like any other contractor. The situation is not materially different in instances where accreditation from a private organization would have the effect of ''deeming'' the covered entity to be in compliance with a government standard or condition of participation in a government program. In both cases, the accreditation organization is performing a service for the covered entity, not for the government. In our considerations, we were unable to identify a reason that covered entities should hold these contractors to lesser standards than their other contractors. Individuals' privacy interests would not be diminished in this situation, nor is there any reason why such accreditation organizations should not be held to the requirements described above for business partners. Proposed rules for disclosure to these entities are discussed in section II.C.5., ''Application to business partners.'' We invite comment on our proposed approach.

c. *Additional considerations.* We do not propose any new administrative or judicial process prior to disclosure. This regulation would permit disclosure of protected health information without compulsory process where such disclosure is otherwise allowed. However, this regulation also would not abrogate or modify other statutory requirements for administrative or judicial determinations or for other procedural safeguards, nor would it permit disclosures forbidden by other law.

Under this § 164.518(c), covered entities would have an obligation to verify the identity of the person requesting protected health information and the legal authority behind the request before the disclosure would be permitted under this subsection. Preamble section II.G.3. describes these requirements in more detail.

3. Use and Disclosure for Judicial and Administrative Proceedings (§ 164.510(d))

[*Please label comments about this section with the subject: ''Judicial and administrative proceedings''*]

In § 164.510(d), we propose to permit covered entities to disclose protected health information in a judicial or administrative proceeding if the request for such protected health information is made through or pursuant to an order by a court or administrative tribunal. A court order would not be required if the protected health information being requested relates to a party to the proceeding whose health condition is at issue, or if the disclosure would otherwise be permitted under this rule. A covered entity that also is a government entity would be permitted to use protected health information in a judicial or administrative proceeding under the same conditions that it could make a disclosure of protected health information under this paragraph.

a. *Importance of judicial and administrative process and the need for protected health information.* Protected health information is often needed as part of an administrative or judicial proceeding. Examples of such proceedings would include personal injury or medical malpractice cases or other lawsuits in which the medical condition of a person is at issue, and judicial or administrative proceedings to determine whether an illness or injury was caused by workplace conditions or exposure to environmental toxins. The information may be sought well before a trial or hearing, to permit the party to discover the existence or nature of testimony or physical evidence, or in conjunction with the trial or hearing, in order to obtain the presentation of testimony or other evidence. These uses of health information are clearly necessary to allow the smooth functioning of the legal system. Requiring the authorization of the subject prior to disclosure could mean that crucial information would not be available, and could be unfair to persons who have been wronged.

b. *Proposed requirements.* We propose to permit covered entities to disclose protected health information in a judicial or administrative proceeding if the request for such protected health information is made through or pursuant to a court order or an order by an administrative law judge specifically authorizing the disclosure of protected health information. The exception to this requirement is where the protected health information being requested relates to a party to the proceeding whose health condition is at issue, and where the disclosure is made pursuant to lawful process (e.g., a discover order) or is otherwise authorized by law. We note that this would not apply where the disclosure would otherwise be permitted under this rule.

The proposed provisions of this section are intended to apply to the broad spectrum of judicial and administrative procedures by which litigants, government agencies, and others request information for judicial or administrative proceedings, including judicial subpoenas, subpoenas duces tecum, notices of deposition, interrogatories, administrative subpoenas, and any disclosure pursuant to the Federal Rules of Civil Procedures, the Federal Rules of Criminal Procedures, comparable rules of other courts (including State, tribunal, or territorial courts) and comparable rules of administrative agencies. Under the rule, a covered entity could not respond to such requests unless they determined that the request is pursuant to a court order authorizing disclosure of protected health information or if the individual who is the subject of the protected health information is a party to the proceeding and his or her medical condition or history is at issue.

Covered entities generally would not be required to conduct any independent investigation of the legality of the process under which the protected health information is being sought, but would need to review the request protected health information to ensure that the disclosure would meet the terms of this provision. Where the request is accompanied by an order from a court, the covered entity could rely on a statement in the order authorizing disclosure of protected health information. The statement could be a general one, indicating that protected health information is relevant to the matter, or it could identify specifically what protected health information may be disclosed. The covered entity could rely on either type of statement, but it could not disclose more information than was authorized by the court where the scope of the authorized disclosure is clear.

Where the request is not accompanied by a court order or order from an administrative law judge, the covered entity would be required to determine whether the request relates to the protected health information of a litigant whose health is at issue, a written statement from the requester certifying that the protected health information being requested is about a litigant to the proceeding and that the health condition of such litigant is at issue at such proceeding. Such a certification could be from the agency requesting the information (e.g., in an administrative proceeding) or from legal counsel representing a party to litigation. We invite comments on whether this requirement is overly burdensome and on whether it is sufficient to protect protected health information from unwarranted disclosures.

We are not proposing to preclude a covered entity from contesting the nature or scope of the process when the procedural rules governing the proceeding so allow and covered entities could well choose to assert privileges against disclosure on behalf of individuals.

In developing our proposal, we considered permitting covered entities to disclose protected health information pursuant to any request made in conjunction with a judicial or administrative proceeding. We rejected this option because we believe that current procedures for document production could result in unwarranted disclosure of protected health information. Under current practice, requests for documents are developed by the parties to a proceeding, with little review or oversight unless the request is challenged by the opposing party. In many instances, the parties make very broad discovery requests that result in the production of large numbers of documents for review. Recipients of broad motions for document production often provide the requester with a substantial quantity of material, expecting the requester to page through the documents to identify the ones that are relevant to the proceeding. While such a process may be appropriate for many types of records, we are concerned that it could lead to substantial breaches of privacy where the material being requested is protected health information. We are unsure if it is appropriate for private attorneys, government officials and others who develop such requests to be able to circumvent the protections provided by this rule with simple motions for document production that have not been subject to third-party review.

Under our proposal, therefore, a party to a proceeding that wishes production of information that includes protected health information would generally need to seek judicial review of the request. If a court determines that a request for protected health information is appropriate to the proceeding, a covered entity can produce the protected health information pursuant to an otherwise lawful request.

We propose an exception to the general requirement for judicial review for protected health information for instances in which the protected health information of a party to the proceeding is relevant to the proceeding. In such instances, the party will have counsel who can object to an overly broad or unwarranted discovery of the party's protected health information or will receive the discovery request directly and, again, will have an opportunity to object prior to disclosure.

We note that there are other existing legal requirements governing the disclosure of protected health information, and which govern the procedures in federal, State and other judicial and administrative proceedings. For example, 42 U.S.C. 290dd–2 and the implementing regulations, 42 CFR part 2, will continue to govern the disclosure of substance abuse patient records. There may also be provisions of a particular State's law governing State judicial or administrative proceedings, including State medical record privacy statutes, as well as precedential court opinions, which apply to the circumstances described in the section, that will not be preempted by this part. Also, the discovery of psychiatric counseling records in federal proceedings governed by section 501 of the Federal Rules of Evidence, has been restricted in certain circumstances, by *Jaffee* v. *Redmond*, 116 S. Ct. 1923 (1996). These more stringent rules would remain in place.

4. Disclosure to Coroners and Medical Examiners (§ 164.510(e))

[*Please label comments about this section with the subject: ''Coroners and medical examiners''*]

In § 164.510(e), we propose to allow covered entities to disclose protected health information without individual authorization to coroners and medical examiners, as authorized by law, for identification of a deceased person or to determine cause of death.

a. Importance of disclosure to coroners and medical examiners and the need for protected health information. Coroners and medical examiners, who under State or other law typically are public officials, have a legitimate need to obtain protected health information in an expeditious manner in order to carry out their legal responsibility to identify deceased persons and determine cause of death. Such disclosure would be clearly in the public interest, and should be included among the types of disclosures for which the public interest in efficient sharing of medical information outweighs any individual privacy interests that may be compromised.

b. *Proposed requirements.* Proposed § 164.510(e) would allow covered entities to disclose protected health information about a deceased person without individual authorization to coroners and medical examiners, consistent with other law, for the purpose of a post-mortem investigation.

We recognize that a deceased person's medical record could include information that potentially could reveal health information about others, for example, relatives who have the same genetically linked disease as the deceased individual. In developing this section of the proposed rule, we considered requiring covered entities to redact any protected health information about persons other than the deceased before giving the record to coroners or medical examiners.

We rejected this option for two reasons. First, coroners and medical examiners typically need significant portions of a deceased person's medical record, and, in some cases, all medical records that are available, to conduct a post-mortem investigation, which may also include an autopsy. Second, they need to obtain the record quickly, because there is a limited time period after death within which an autopsy can be conducted. Requiring covered entities to take the time to review and redact portions of the health information before providing it to a coroner or medical examiner would create delays that could make it impossible to conduct an autopsy appropriately. Nothing in this rule would prohibit a covered entity from undertaking such redaction on its own initiative so long as the information provided would meet the needs of the coroner or medical examiner.

In addition to these two reasons, it is our understanding that health care providers, as a standard record keeping practice, rarely identify specific persons other than the patient in the record. We are soliciting comment on whether health care providers routinely identify other persons specifically in a individual's record and if so, whether we should require the provider to redact the information about the other person before providing it to a coroner or medical examiner.

Under § 164.518(c), covered entities would have an obligation to verify the identity of the coroner or medical examiner making the request for protected health information and the legal authority supporting the request, before the disclosure would be permitted under this subsection. Preamble section II.G.3. describes these requirements in more detail.

We intend to allow only those disclosures that are authorized by other applicable law. Laws vary widely regarding release of health information to coroners and medical examiners for the purposes of identifying deceased persons or determining cause of death, and we do not intend to disturb those practices.

5. Disclosure for Law Enforcement (§ 164.510(f))

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

In § 164.510(f), we propose to permit covered entities to disclose protected health information without individual authorization to a law enforcement official conducting a law enforcement inquiry authorized by law if the request for protected health information is made pursuant to a judicial or administrative process, as described below. Similarly, we propose to permit covered entities to disclose protected health information to a law enforcement official without individual authorization for the conduct of lawful intelligence activities. We also propose to permit covered entities to disclose protected health information to a law enforcement official about the victim of a crime, abuse or other harm, if the information is needed to determine both whether a violation of law by a person other than the victim has occurred and whether an immediate law enforcement activity might be necessary. We would further permit such disclosure for the purpose of identifying a suspect, fugitive, material witness, or missing person, if the covered entity discloses only limited identifying information. Finally, we would permit disclosure of protected health information by a health plan or a health care provider without individual authorization to law enforcement officials if the plan or provider believed in good faith that the disclosed protected health information would constitute evidence of criminal conduct that constitutes health care fraud, occurred on the premises of the covered entity, or was witnessed by an employee of the covered entity.

i. *Law enforcement need for protected health information.* Law enforcement officials need protected health information for their investigations in a variety of circumstances. Health information about a victim of a crime may be needed to investigate the crime, or to allow prosecutors to determine the proper charge. For some crimes, the severity of the victim's injuries will determine what charge should be brought against a suspect. The medical condition of a defendant could also be relevant to whether a crime was committed, or to the seriousness of a crime. The medical condition of a witness could be relevant to the reliability of that witness. Medical, billing, accounting or other documentary records in the possession of a covered entity can be important evidence relevant to criminal fraud or conspiracy investigations. Nor is this list of important uses by law enforcement exhaustive.

In many cases, the law enforcement official will obtain such evidence through legal process, such as judicially executed warrant, an administrative subpoena, or a grand jury subpoena. In other circumstances, time constraints preclude use of such process. For example, health information may be needed when a law enforcement official is attempting to apprehend an armed suspect who is rapidly fleeing. Health information may be needed from emergency rooms to locate a fleeing prison escapee or criminal suspect who was injured and is believed to have stopped to seek medical care.

Protected health information could be sought as part of a law enforcement investigation, to determine whether and who committed a crime, or it could be sought in conjunction with the trial to be presented as evidence. These uses of medical information are clearly in the public interest. Requiring the authorization of the subject prior to disclosure could impede important law enforcement activities by making apprehension and conviction of some criminals difficult or impossible.

As described above, this proposed rule seeks to respond appropriately to new risks to privacy that could emerge as the form of medical records changes in coming years. The administrative simplification mandated by HIPAA will lead to far greater exchanges of individually identifiable health information among covered entities in the future, increasingly in electronic form. If a misperception were to develop that law enforcement had instant and pervasive access to medical records, the goals of this proposed regulation could be undermined. For instance, individuals might become reluctant to seek needed care or might report inaccurately to providers to avoid revealing potentially embarrassing or incriminating information. In addition, popular concerns about government access to sensitive medical records might impede otherwise achievable progress toward administrative simplification. We believe that the proposed prophylactic and administrative rules governing disclosure to law enforcement officials, as described below, are justified in order to avoid these harms in the future.

ii. *Proposed requirements.* In § 164.510(f), we propose to permit covered entities to disclose protected health information to law enforcement officials conducting or supervising a law enforcement inquiry or proceeding authorized by law if the request for protected health information is made:

- Pursuant to a warrant, subpoena, or order issued by a judicial officer;
- Pursuant to a grand jury subpoena;
- Pursuant to an administrative subpoena or summons, civil investigative demand, or similar certification or written order issued pursuant to federal or state law where (i) the records sought are relevant and material to a legitimate law enforcement inquiry; (ii) the request is as specific and narrowly drawn as is reasonably practicable to meet the purposes of the inquiry; and (iii) de-identified information could not reasonably be used to meet the purposes of the inquiry;
- For limited identifying information where necessary to identify a suspect, fugitive, witness, or missing person;
- By a law enforcement official requesting protected health information about an individual who is, or who is suspected to be, the victim of a crime, abuse or other harm, if such law enforcement official represents that (i) such information is needed to determine whether a violation of law by a person other than the victim has occurred and (ii) immediate law enforcement activity which depends on the official obtaining such information may be necessary;
- For the conduct of lawful intelligence activities conducted pursuant to the National Security Act of 1947 (50 U.S.C. 401 *et seq.*) or in connection with providing protective services to the President or other individuals pursuant to section 3056 of title 18, United States Code, and the disclosure is otherwise authorized under Federal or state law; or
- To law enforcement officials when a covered entity believes in good faith that the disclosed protected health information constitutes evidence of criminal conduct that: (i) Arises out of and is directly related to the receipt of health care or payment for health care (including a fraudulent claim for health care) or qualification for or receipt of benefits, payments or services based on a fraudulent statement or material misrepresentation of the health of a patient; (ii) occurred on the premises of the covered entity; or (iii) was witnessed by an employee or other workforce member of the covered entity.

In drafting the proposed rule, we have attempted to match the level of procedural protection for privacy with the nature of the law enforcement need for access. Therefore, access for law enforcement under this rule would be easier where other rules would impose procedural protections, such as where access is granted after review by an independent judicial officer. Access would also be easier in an emergency situation or where only limited identifying information would be provided. By contrast, this rule proposes stricter standards for administrative requests, where other rules could not impose appropriate procedural protections.

Under the first part of this proposal, we would authorize disclosure of protected health information pursuant to a request that has been reviewed by a judicial officer. Examples of such requests include State or federal warrants, subpoenas, or other orders signed by a judicial officer. Review by a judicial officer is significant procedural protection for the proper handling of individually identifiable health information. Where such review exists, we believe that it would be appropriate for covered entities to disclose individually identifiable health information pursuant to the order.

Under the second part of this proposal, we would authorize disclosure of protected health information pursuant to a State or federal grand jury subpoena. Information disclosed to a grand jury is covered by significant secrecy protections, such as under Federal Rule of Criminal Procedure 6(e) and similar State laws. Our understanding is that State grand juries have secrecy protections substantially as protective as the federal rule. We solicit comment on whether there are any State grand jury secrecy provisions that are not substantially as protective.

Under the third part of this proposal, we would set somewhat stricter standards than exist today for disclosure pursuant to administrative requests, such as an administrative subpoena or summons, civil investigative demand, or similar process authorized under law. These administrative actions do not have the same procedural protections as review by an independent judicial officer. They also do not have the grand jury secrecy protections that exist under federal and State law. For administrative requests, an individual law enforcement official can define the scope of the request, sometimes without any review by a superior, and present it to the covered entity. We propose, therefore, that a greater showing should be made for an administrative request before the covered entity would be permitted to release protected health information. We also believe that the somewhat stricter test for administrative requests would provide some reason for officials to choose to obtain protected health information through process that includes the protections offered by judicial review or grand jury secrecy.

We therefore propose that a covered entity could disclose protected health information pursuant to an administrative request, issued pursuant to a determination that: (i) The records sought are relevant and material to a legitimate law enforcement inquiry; (ii) the request is as specific and narrowly drawn as is reasonably practicable; and (iii) de-identified information could not reasonably be used to meet the purpose of the request.

Because our regulatory authority does not extend to law enforcement officials, we are seeking comment on how to create an administrable system for implementing this three-part test. We do not intend that this provision require a covered entity to second guess representations by an appropriate law enforcement official that the three part test has been met.

To verify that the three-part test has been met, we propose that a covered entity be permitted to disclose protected health information to an appropriate law enforcement official pursuant to a subpoena or other covered administrative request that on its face indicates that the three-part test has been met. In the alternative, where the face of the request does not indicate that the test has been met, a covered entity could disclose the information upon production of a separate document, signed by a law enforcement official, indicating that the three-part test has been met. Under either of these alternatives, disclosure of the information can also be made if the document applies any other standard that is as strict or stricter than the three-part test.

This approach would parallel the research provisions of proposed § 164.510(j). Under that section, disclosure would be authorized by a covered entity where the party seeking the records produces a document that states it has met the standards for the institutional review board process. We solicit comments on additional, administrable ways that a law enforcement official could demonstrate that the appropriate issuing authority has determined that the three-part test has been met.

We solicit comment on the burdens and benefits of the proposed three-part test for administrative requests. For covered entities, we are interested in comments on how burdensome it would be to determine whether the three-part test has been met, and we would explore suggestions for approaches that would be more easily administered. For law enforcement, we are interested in the potential impact that this approach might have on current law enforcement practices, and the extent to which law enforcement officials believe that their access to information critical to law enforcement investigations could be impaired. We solicit comment on the burden on law enforcement officials, compared to current practice, of writing the administrative requests. We would also like comments on whether there are any federal, State, or local laws that would create an impediment to application of this section, including the proposed three-part test. If there are such impediments, we would solicit comment on whether extending the effective date of this section could help to prevent difficulties. On the benefit side, we are interested in comments on the specific gains for privacy that would result from requiring law enforcement to comply with greater procedures than currently exist for gaining access to protected health information.

As the fourth part of this proposal, we address limited circumstances where the disclosure of health information by covered entities would not be made pursuant to lawful process such as judicial order, grand jury subpoena, or administrative request. In some cases law enforcement officials could seek limited but focused information needed to obtain a warrant. For example, a witness to a shooting may know the time of the incident and the fact that the perpetrator was shot in the left arm, but not the identity of the perpetrator. Law enforcement would then have a legitimate need to ask local emergency rooms whether anyone had presented with a bullet wound to the left arm near the time of the incident. Law enforcement may not have sufficient information to obtain a warrant, but instead would be seeking such information. In such cases, when only limited identifying information is disclosed and the purpose is solely to ascertain the identity of a person, the invasion of privacy would be outweighed by the public interest.

In such instances, we propose to permit covered entities to disclose ''limited identifying information'' for purposes of identifying a suspect, fugitive, material witness, or missing person. We would define ''limited identifying information'' as the name, address, social security number, date of birth, place of birth, type of injury, date and time of treatment, and date of death. Disclosure of any additional information would cause the covered entity to be out of compliance with this provision, and subject to sanction. The request for such information could be made orally or in writing. Requiring the request to be in writing could defeat the purposes of this provision. We solicit comment on whether the list of ''limited identifying information'' is appropriate, or whether additional identifiers, such as blood type, also should be permitted disclosures under this section. Alternatively, we solicit comment on whether any of the proposed items on the list are sufficiently sensitive to warrant a legal process requirement before they should be disclosed.

Under the fifth part of the proposal, we would clarify that the protected health information of the victim of a crime, abuse or other harm could be disclosed to a law enforcement official if the information is needed to determine both whether a violation of law by a person other than the victim has occurred and whether an immediate law enforcement activity might be necessary. There could be important public safety reasons for obtaining medical records or other protected health information quickly, perhaps before there would be time to get a judicial order, grand jury subpoena, or administrative order. In particular, where the crime was violent, information about the victim's condition could be needed to present to a judge in a bond hearing in order to keep the suspect in custody while further evidence is sought. Information about the victim also could be important in making an appropriate charging decision. Rapid access to victims' medical records could reduce the risk of additional violent crimes, such as in cases of spousal or child abuse or in situations where the protected health information could reveal evidence of the identity of someone who is engaged in ongoing criminal activities.

In some of these instances, release of protected health information would be authorized under other sections of this proposed regulation, pursuant to provisions for patient consent, health oversight, circumstances, or disclosure pursuant to mandatory reporting laws for gunshot wounds or abuse cases. (As discussed later in section II.I, our rule would not be construed to invalidate or limit the authority, powers or procedures established under any law that provides for reporting of injury, child abuse or death.) In addition, § 164.510(k) addressing emergency circumstances would permit covered entities to disclose protected health information in instances where the disclosure could prevent imminent harm to the individuals or to the public. However, we propose to include this fifth provision for law enforcement access to ensure that immediate need for law enforcement access to information about a victim would be permitted under this rule.

Under the sixth part of this proposal, we seek to assure that this rule would not interfere with the conduct of lawful security functions in protection of the public interest, as defined by the Congress. Therefore, we would allow disclosure of protected health information for the conduct of lawful intelligence activities conducted pursuant to the National Security Act of 1947. Similarly, we would allow disclosure of protected health information for providing protective services to the President or other individuals pursuant to section 3056 of title 18, United States Code. Where such disclosures are authorized by Federal or state law, we would not interfere with these important national security activities.

Under the final part of this proposal, we would permit covered entities that uncover evidence of health care fraud to disclose the protected health information that evidences such fraud to law enforcement officials without receiving a request from such officials. This provision would permit covered entities to make certain disclosures to law enforcement officials on their own initiative if the information disclosed constitutes evidence of criminal conduct that arises out of and is directly related to (i) the receipt of health care or payment for health care (including a fraudulent claim for health care) or (ii) qualification for or receipt of benefits, payments or services based on a fraudulent statement or material misrepresentation of the health of a patient. Similarly, we would permit covered entities on their own initiative to disclose to law enforcement officials protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that either occurred on the covered entity's premises or was witnessed by an employee (or other workforce member) of the covered entity. In such situations, covered entities should be permitted to take appropriate steps to protect the integrity and safety of their operations or to assure that the such criminal conduct is properly prosecuted.

To be protected by this provision, the covered entity would have to have good faith belief that the disclosed protected health information was evidence of such conduct. If the covered entity disclosed protected health information in good faith but was wrong in its belief that the information evidenced a legal violation, the covered entity would not be subject to sanction under this regulation. We would not require the covered entity to accurately predict the outcome of a criminal investigation.

There also are situations where law enforcement officials would need access to information for emergency circumstances. In those cases, the disclosure could be made under § 164.510(k), ''Disclosure in emergency circumstances.''

Pursuant to § 164.518(c), covered entities would have an obligation to verify the identity of the person seeking disclosure of protected health information and the legal authority behind the request. As described in section II.H.3. of this preamble, we would permit covered entities to rely on a badge or similar identification to confirm that the request for protected health information is being made by a law enforcement official. If the request is not made in person, we would permit the covered entity to rely on official letter head or similar proof.

Where the covered entity must verify that lawful process has been obtained, § 164.518(c) would require the covered entity to review the document evidencing the order. The covered entity could not disclose more information than was authorized in the document.

Because the regulation applies to covered entities, and not to the law enforcement officials seeking the protected health information, the covered entity would not be in a position to determine with any certainty whether the underlying requirements for the process have been met. For instance, it may be difficult for the covered entity to determine whether the three-part test has been met for an administrative request. In light of this difficulty facing covered entities, the proposed rule would include a good faith provision. Under that provision, covered entities would not be liable under the rule for disclosure of protected health information to a law enforcement official where the covered entity or its business partners acted in a good faith belief that the disclosure was permitted under this title. We solicit comment on the extent to which this good faith provision would make the proposed rule less burdensome on covered entities and law enforcement officials. We also solicit comment on the extent to which the provision could undermine the effectiveness of the provision.

For requests for the conduct of intelligence activities or for protective services, covered entities would be required to verify the identity of the person or entity requesting the information, through a badge or other identification, or official letter head, as just described. If such verification of identity is obtained, covered entities would be permitted to reasonably rely on the representations of such persons that the request is for lawful national security or protective service activities and is authorized by law. Similarly, to disclose limited identifying information, covered entities would be required to obtain verification that the request comes from a law enforcement official, and would be permitted to reasonably rely on such official's representation that the information is needed for the purpose of identifying a suspect, fugitive, material witness, or missing person and is authorized by law.

iii. *Additional considerations.* This section is not intended to limit or preclude a covered entity from asserting any lawful defense or otherwise contesting the nature or scope of the process when the procedural rules governing the proceeding so allow, although it is not intended to create a basis for appealing to federal court concerning a request by state law enforcement officials. Each covered entity would continue to have available legal procedures applicable in the appropriate jurisdiction to contest such requests where warranted. This proposed rule would not create any new affirmative requirement for disclosure of protected health information. Similarly, this section is not intended to limit a covered entity from disclosing protected health information for law enforcement purposes where other sections of the rule permit such disclosure, e.g., as permitted by § 164.510 under emergency circumstances, for oversight or public health activities, to coroners or medical examiners, and in other circumstances permitted by the rule.

In obtaining protected health information, law enforcement officials would have to comply with whatever other law was applicable. In certain circumstances, while this subsection could authorize a covered entity to disclose protected health information to law enforcement officials, there could be additional applicable statutes that further govern the specific disclosure. If the preemption provisions of this regulation do not apply, the covered entity must comply with the requirements or limitations established by such other law, regulation or judicial precedent. See proposed §§ 160.201 through 160.204. For example, if State law would permit disclosure only after compulsory process with court review, a provider or payer would not be allowed to disclose information to state law enforcement officials unless the officials had complied with that requirement. Similarly, disclosure of substance abuse patient records subject to, 42 U.S.C. 290dd–2, and the implementing regulations, 42 CFR part 2, would continue to be governed by those provisions.

In some instances, disclosure of protected health information to law enforcement officials would be compelled by other law, for example, by compulsory judicial process or compulsory reporting laws (such as laws requiring reporting of wounds from violent crimes, suspected child abuse, or suspected theft of prescription controlled substances). Disclosure of protected health information under such other mandatory law would be permitted under proposed § 164.510(n).

In developing our proposal, we considered permitting covered entities to disclose protected health information pursuant to any request made by a law enforcement official, rather than requiring some form of legal process or narrowly defined other circumstances. We rejected this option because we believe that in most instances some form of review should be required. Individuals' expectation of privacy with respect to their health information is sufficiently strong to require some form of process prior to disclosure to the government. At the same time, we recognize that the public interest would not be served by requiring such formal process in every instance. Under our proposal, therefore, law enforcement could obtain certain identifying information in order to identify suspects and witnesses, and could obtain information for national security or protective services activities or in emergency circumstances. Similarly, we would not require process before a law enforcement official could obtain information about the victim of a crime, where the information is necessary as the basis for immediate action. In addition, in seeking an appropriate balance between public safety and individuals' expectation of privacy, we are proposing that covered entities not be subject to enforcement under this regulation if they disclose protected health information to law enforcement officials in a good faith belief that the disclosure was permitted under this title.

We solicit comment on what additional steps, if any, are appropriate for allowing law enforcement access to protected health information. We are interested in comments concerning situations where needed access to protected health information would not be available under these or other provisions of this proposed rule. We also seek comment on specific privacy or other concerns that would apply if the final regulation included provision for law enforcement access to protected health information without requiring a judicial order, grand jury subpoena, or administrative request, under such additional defined circumstances.

In some of these instances, release of protected health information would be authorized under the proposed regulation pursuant to provisions for patient consent, health oversight, emergency circumstances, or under mandatory reporting laws for gunshot wounds or abuse cases. We are interested in comments concerning situations where needed access to protected health information would not be available under these or other provisions of this proposed rule. We also seek comment on specific privacy or other concerns that would apply if the final regulation included provision for law enforcement access to protected health information without requiring a judicial order, grand jury subpoena, or administrative request, under such additional defined circumstances.

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

6. Uses and Disclosures for Governmental Health Data Systems (§ 164.510(g))

[*Please label comments about this section with the subject: ''Governmental health data systems''*]

In § 164.510(g), we propose to permit covered entities to disclose protected health information for inclusion in State or other governmental health data systems without individual authorization when such disclosures are authorized by State or other law in support of policy, planning, regulatory or management functions.

a. *Importance of Governmental health data systems and the need for protected health information.* Governmental agencies collect and analyze individually identifiable health information as part of their efforts to improve public policies and program management, improve health care and reduce costs, and improve information available for consumer choices. Governments use the information to analyze health care outcomes, quality, costs and patterns of utilization, effects of public policies, changes in the health care delivery system, and related trends. These important purposes are related to public health, research and oversight (although the information in State or other governmental data systems usually is not collected specifically to audit or evaluate health care providers or for public health surveillance). The data are an important resource that can be used for multiple public policy evaluations.

The collection of health information by governmental health data systems often occurs without specification of the particular analyses that could be conducted with the information. These governmental data collection programs frequently call for reporting of information for all individuals treated or released by specified classes of providers. For example, many States request and receive from hospitals records containing individual diagnosis and treatment data for all discharges from their facilities. State hospital discharge data have been used to compare treatment practices and costs between hospitals, to evaluate implications for funding of health care, as well as to provide hospital ''report cards'' to consumers. As part of its general evaluation activities, the DOD maintains a very large database, called the Comprehensive Clinical Evaluation Program, involving military personnel who have reported illnesses possibly arising from service during the Gulf War.

b. *Proposed requirements.* We propose to permit covered entities to disclose protected health information for inclusion in State or other governmental health data systems when such disclosure is authorized by law for analysis in support of policy, planning, regulatory, and management functions. The recipient of the information must be a government agency (or privacy entity acting on behalf of a government agency). Where the covered entity is itself a government agency that collects health data for analysis in support of policy, planning, regulatory, or management functions, it would be permitted to use protected health information in all cases in which it is permitted to disclose such information for government health data systems under this section.

We believe that Congress intended to permit States, Tribes, territories, and other governmental agencies to operate health data collection systems for analyzing and improving the health care system. In section 1178(c), ''State regulatory reporting,'' HIPAA provides that it is not limiting the ability of a State to require a health plan to report, or to provide access to, information for a variety of oversight activities, as well as for ''program monitoring and evaluation.'' We also believe that the considerations Congress applied to State capacities to collect data would apply to similar data collection efforts by other levels of government, such as those undertaken by Tribes, territories and federal agencies. Therefore, we considered two questions regarding governmental health data systems; first, which entities could make such disclosures; and second, what type of legal authority would be necessary for the disclosure to be permitted.

We considered whether to allow disclosure by all covered entities to governmental data collection systems or to limit permitted disclosures to those made by health plans, as specified in the regulatory reporting provision of HIPAA. While this provision only mentions data collected from health plans, the conference agreement notes that laws regarding ''State reporting on health care delivery or costs, or for other purposes'' should not be preempted by this rule. States would be likely to require sources of information other than health plans, such as health care providers or clearinghouses, in order to examine health care delivery or costs. Therefore, we do not believe it is appropriate to restrict States' or other governmental agencies' ability to obtain such data. This viewpoint is consistent with the Recommendations, which would permit this disclosure of protected health information by all covered entities.

We also asked what type of law would be required to permit disclosure without individual authorization to governmental health data systems. We considered requiring a specific statute or regulation that requires the collection of protected health information for a specified purpose. A law that explicitly addresses the conditions under which protected health information is collected would provide individuals and covered entities with a better understanding of how and why the information is to be collected and used.

We understand, however, that explicit authority to collect information is not always included in relevant law. Governmental agencies may collect health data using a broad public health or regulatory authority in statute or regulation. For example, a law may call on a State agency to report on health care costs, without providing specific authority for the agency to collect the health care cost data they need do so. Consequently, the agency may use its general operating authority to request health care providers to release the information. We recognize that many governmental agencies rely on broad legal authority for their activities and do not intend this proposed rule to hamper those efforts.

Under § 164.518(c), covered entities would have an obligation to verify the identity of the person requesting protected health information, and the legal authority behind the request before the disclosure would be permitted under this subsection. Preamble section II.G.3. describes these requirements in more detail.

7. Disclosure of Directory Information (§ 164.510(h))

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

In § 164.510(h), we propose to permit covered entities to disclose information that could reveal protected health information about an individual for purposes of a facility patient directory, if the individual has indicated consent to such disclosures, or if the individual who is incapacitated had not previously expressed a preference in this regard and a covered entity determines that including such information in the directory would be consistent with good medical practice. Directory information could include only the person's name, location in the institution, and general condition.

a. *Importance of directory information and need for protected health information.* When individuals enter inpatient facilities, they are not always able to contact people who may need to know their whereabouts, want to visit them, or want to send them flowers or some other expression of concern. Today, facilities typically operate patient directories, allowing confirmation of a person's presence in a facility, providing the room number for visits and deliveries, and sometime providing general information on the patient's condition. These services cannot be performed without disclosing protected health information. Since most patients find this a welcome convenience, we believe it would be important to allow these practices to continue. However, not everyone may appreciate this service. We are proposing to accommodate the wishes of such people, where possible.

b. *Proposed requirements.* In § 164.510(h), we would require covered entities to ask individuals whether they wish to be included in the entity's directory. For individuals who are incapacitated or otherwise unable to communicate their wishes and who have not previously expressed a preference, the decision would be left to the discretion of the covered entity, consistent with good medical practice. We note that legal representatives could make such decisions on behalf of persons who are incapacitated or otherwise unable to communicate their wishes, consistent with State or other law, since they would stand as the ''individual.'' In the absence of a legal representative or prior expression of a preference by the individual, the decision would be left to the discretion of the covered entity, consistent with good medical practice.

i. *Individuals capable of making decisions.*

For individuals who are not incapacitated, this rule would require the covered entity to ask whether information about the individual's presence in the facility, room number and general condition can be included in the general patient directory. When individuals are capable of making such a determination, their wishes should be respected.

We considered whether also to require covered entities to allow an individual to specify that information can be provided to specific persons but not others. For example, someone may feel that it is acceptable to release information to family members but not to friends. While we would like to respect individuals' wishes to the greatest extent possible, we are concerned about placing on covered entities the burden of verifying the identify of a person requesting directory information. We are therefore not including this additional requirement, but are requesting comments on current practices and how such requests might be accommodated.

We would not require a formal individual authorization pursuant to § 164.508. A verbal or other informal inquiry and agreement would be sufficient. We require only that individuals be given the choice.

ii. *Incapacitated individuals.*

If an individual is not able to make determinations as to whether location or status information should be released to family and friends, and had not in the past expressed a preference in this regard, we would leave the decision as to whether to include the individual in a directory to the discretion of the covered entity. Often individuals are unconscious or otherwise unable due to a medical condition to communicate their wishes to the entity and no representative is available to act for them. In these cases, we encourage the covered entity to take into consideration a number of factors when deciding whether or not to include such an individual in the directory:

- Could disclosing that an individual is in the facility reasonably cause danger of harm to the individual? For example, if a person is unconscious and receiving treatment for injuries resulting from physical abuse from an unknown source, an entity may determine that revealing that the individual is in the facility could give the attacker enough information to seek out the individual and repeat the abuse.

• Could disclosing the location within the facility of the patient give information about the condition of the patient? If a patient's room number would reveal the nature of the medical condition, the entity may decide that it is inappropriate to give that information. For example, if one floor of a hospital has been specifically designated as the psychiatric floor, simply saying that a patient is located on that floor discloses some information about the condition of the individual.

• Is it necessary or appropriate to give the status of a patient to family or friends? Covered entities often need information from family or friends for the treatment of an incapacitated individual. For example, if a patient is unconscious, family or friends may be able to give valuable information that will assist the care giver in making urgent decisions. Family members or friends may be able to give information on drugs or medications that the individual has been taking. On the other hand, it may be that revealing the status of an individual gives more information than the individual would have disclosed if they could make the determination themselves.

• If an individual had, prior to becoming incapacitated, expressed a desire not to be included in such a directory and the covered entity learns of that statement of preference, the covered entity would be required to act in accordance with the stated preference.

Individuals who enter a facility incapacitated and then improve to the point of being able to make their own determinations should be asked within a reasonable time period for permission to include information in the facility's directory.

When the condition of an individual who has opted not to allow protected health information to be included in the facility's directory deteriorates, and the individual is no longer capable of making disclosure decisions, the covered entity would be required to abide by the individual's initial decision. However, such a decision should not prevent a provider from contacting the family if such contact is required for good medical practice. A provider could need information from the family to treat a newly incapacitated person. If good medical practice would include contacting family or friends, the individual's initial request should not prohibit such contact. But the covered entity would still be prohibited from including information about the individual in its directory.

8. Disclosure for Banking and Payment Processes (§ 164.510(i))

[*Please label comments about this section with the subject: ''Banking and payment processes''*]

In § 164.510(i), we propose to allow covered entities to disclose protected health information to financial institutions, or entities acting for financial institutions, if necessary for processing payments for health care and health care premiums.

a. *Importance of financial transactions and the need for protected health information.* Checks that individuals use to pay for health care typically include the names of providers or provider groups that could implicitly identify the medical condition for which treatment was rendered. Similarly, a credit card transaction will also reveal the identify of the provider and thus potentially the nature of the medical condition involved. While such information would constitute protected health information under this rule, there is no practical way of concealing this information when the provider deposits the check or claims credit card payment. Failure to allow this kind of disclosure of protected health information would impede the efficient operations of the health care system.

b. *Proposed requirements.* We propose that covered entities be permitted to disclose protected health information to financial institutions for the specific purposes listed in the section. The permissible purposes are those identified in the statute, and the regulatory text would copy the statutory list of allowable uses.

Under section 1179 of the Act, activities of financial institutions are exempt from HIPAA's Administrative Simplification requirements to the extent that those activities constitute ''authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments'' for health care or health plan premiums. This section of the statute states that financial institutions can use or disclose protected health information for these purposes. We read this part of the statute as indicating that Congress intended that this regulation not impede the efficient processing of these transactions, and accordingly are allowing covered entities to disclose protected health information to financial institutions for the purposes listed in section 1179 of the statute.

Proposed § 164.510(i) would not allow covered entities to include any diagnostic or treatment information in the data transmitted to financial institutions. Such information is never necessary to process a payment transaction. We believe that, in most cases, the permitted disclosure would include only: (1) The name and address of the account holder; (2) the name and address of the payer or provider; (3) the amount of the charge for health services; (4) the date on which health services were rendered; (5) the expiration date for the payment mechanism, if applicable (i.e., credit card expiration date); and (6) the individual's signature. At this time, we are not proposing to include in the regulation an exclusive list of information that could be lawfully disclosed for this purpose. We are, however, soliciting comment on whether more elements would be necessary for these banking and payment transactions and on whether including a specific list of the protected health information that could be disclosed is an appropriate approach.

We understand that financial institutions may also provide covered entities that accept payment via credit card with software that, in addition to fields for information required to process the transaction, includes blank fields in which health plans or health care providers may enter any type of information regarding their patients, such as diagnostic and treatment information, or other information that the covered entity wished to track and analyze. Other financial institutions could provide services to covered entities that constitute ''health care operations'' as defined in proposed § 164.504.

We do not know whether and to what extent health plans and health care providers are using such software to record and track diagnostic and treatment and similar information. However, we recognize that the capability exists and that if a plan or provider engages in this practice, information not necessary for processing the payment transaction could be forwarded to financial institutions along with other information used to process payments. Disclosing such information to a financial institution (absent a business partner relationship) would violate the provisions of this rule.

We also understand that banks, in addition to offering traditional banking services, may be interested in offering additional services to covered entities such as claims management and billing support. Nothing in this regulation would prohibit banks from becoming the business partners of covered entities in accordance with and subject to the conditions of § 164.506(e). If a bank offers an integrated package of traditional banking services and health claims and billing services, it could do 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.

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

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.

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 patient demand for access, amendment, and correction of medical records.

Our cost calculations assume that persons who request an opportunity to amend or correct their record have already obtained a copy of their medical record. Therefore, the administrative cost of amending and correcting the patient's record is completely separate from inspection and copying costs. In this section we have only addressed the cost of disputing a factual statement within the patient record, and do not calculate the cost of appeals or third party review.

Administrative review of factual statements contained within a patient's record may be expensive. Most errors may be of a nature that a clerk or nurse can correct (e.g., the date of a procedure is incorrect) but some may require physician review. Thus, we have estimated that the average cost of amending and correcting a patient record may be $75 per instance.

If amendment and correction requests are associated with two-thirds of requests for inspection and copying, and the cost of correcting (or noting the patient's request for correction) is $75, the total cost of amending and correcting patient records will be $407 million annually, or $2 billion over five years. Comments on our estimate of amendment and correction costs would be helpful, particularly if they speak to current amendment and correction costs or frequency in the health care industry.

Reconstructing a History of Disclosures (Other Than for Treatment and Payment)

To our knowledge, no current State law or professional code requires providers and plans to maintain the capability to reconstruct a patient's health information history. Therefore, the requirement in this rule to be able to reconstruct the disclosure history of protected health information is completely new. Although it is likely that some providers and plans have already developed this capability, we assume that all providers and plans would be required to invest in developing the capacity to generate disclosure histories.

With respect to reconstruction of disclosure history, two sets of costs would exist. On electronic records, fields for disclosure reason, information recipient, and date would have to be built into the data system. The fixed cost of the designing the system to include this would be a component of the $90 million additional costs discussed earlier. The ongoing cost would be the data entry time, which should be at de minimis levels. Comments would again be especially useful with respect to the extent to which recording the additional information goes beyond current practice.

Authorizations

Although many States have laws that require entities to obtain patient authorization before releasing individually identified health information to payers and other third parties, many of the authorization requirements either allow for blanket authorizations that deprive the patient of meaningful control over the release of their health information, or the authorization statutes are less stringent than the provisions of the proposed rule. Therefore, for purposes of estimating the economic impact of the NPRM, we are assuming that all providers and plans will have to develop new procedures to conform to the proposed rule.

Written patient authorization requirements will generate costs, to the extent covered entities are currently releasing information in the targeted circumstances without specific authority. Collecting such authorization should have costs on the order of those associated with providing access to records (not on a per page basis). The frequency of such collections is unknown. Since the requirement does not apply to treatment and payment, assuming 1 percent of the 543 million encounters over five years might be reasonable. At a cost of about $10 each, the aggregate cost would be about $54 million annually, or $271 million over five years. Comments would be especially useful from entities currently following such procedures.

Training

The ongoing costs associated with paperwork and training are likely to be minimal. Because training happens as a regular business practice, and employee certification connected to this training is also the norm, we estimate that the marginal cost of paperwork and training is likely to be small. We assume a cost of approximately $20 per provider office, and approximately $60–100 for health plans and hospitals. Thus, we estimate that the total cost of paperwork and training will be $22 million a year.

Conclusion

Overall, the five-year costs beyond those already shown in the administrative simplification estimates would be about $3.8 billion over five years, with an estimated range of $1.8 to $6.3 billion. Table 2 shows the components described above. The largest cost item is for amendment and correction, which is over half of the estimated total cost of the regulation. Inspection and copying, at $405 million over five years, and issuance of notices by providers and plans, at $439 million over five years, are the second biggest components. The one-time costs of development of policies and procedures by providers would represent approximately 10 percent of the total cost, or $333 million. Plans and clearinghouses would have a substantially smaller cost, about $62 million. Other systems changes are expected to cost about $90 million over the period. Finally, the estimates do not consider all of the costs imposed by the regulation.

TABLE 2.—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

TABLE 2.—THE COST OF COMPLYING WITH THE PROPOSED PRIVACY REGULATION—Continued
[In Dollars]

Provision	Initial or first year cost (2000)	Annual cost after the first year	Five year (2000–2004) cost
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''.

Costs to the Federal Government

The proposed rule will have a cost impact on various federal agencies that administer programs that require the use of individual health information. Federal agencies or programs clearly affected by the rule are those that meet the definition of a covered entity. The costs when government entities are serving as providers are included in the total cost estimates. However, non-covered agencies or programs that handle medical information, either under permissible exceptions to the disclosure rules or through an individual's expressed authorization, will likely incur some costs complying with provisions of this rule. A sample of federal agencies encompassed by the broad scope of this rule include the: Department of Health and Human Services, Department of Defense, Department of Veterans Affairs, Department of State, and the Social Security Administration.

The federal costs of complying with the regulation are included in the estimates of total costs. The greatest cost and administrative burden on the federal government will fall to agencies and programs that act as covered entities, by virtue of being either a health plan or provider. Examples include the Medicare, Medicaid, Children's Health Insurance and Indian Health Service programs at the Department of Health and Human Services; the CHAMPVA health program at the Department of Veterans Affairs; and the TRICARE health program at the Department of Defense. These and other health insurance or provider programs operated by the federal government are subject to requirements placed on covered entities under this proposed rule, including, but not limited to, those outlined in Section D of the impact analysis. While many of these federal programs already afford privacy protections for individual health information through the Privacy Act, this rule is expected to create additional requirements beyond those covered by existing Privacy Act rule. Further, we anticipate that most federal health programs will, to some extent, need to modify their existing Privacy Act practices to fully comply with this rule.

The cost to federal programs that function as health plans will be generally the same as those for the private sector. The primary difference is the expectation that systems compliance costs may be higher due to the additional burden of compliance and oversight costs.

A unique cost to the federal government will be in the area of enforcement. The Office of Civil Rights (OCR), located at the Department of Health and Human Services, has the primary responsibility to monitor and audit covered entities. OCR will monitor and audit covered entities in both the private and government sectors, will ensure compliance with requirements of this rule, and will investigate complaints from individuals alleging violations of their privacy rights. In addition, OCR will be required to recommend penalties and other remedies as part of their enforcement activities. These responsibilities represent an expanded role for OCR. Beyond OCR, the enforcement provisions of this rule will have additional costs to the federal government through increased litigation, appeals, and inspector general oversight.

Examples of other unique costs to the federal government include such activities as public health surveillance at the Centers for Disease Control and Prevention, health research projects at the Agency for Health Care Policy and Research, clinical trials at the National Institutes of Health, and law enforcement investigations and prosecutions by the Federal Bureau of Investigations. For these and other activities, federal agencies will incur some costs to ensure that protected health information is handled and tracked in ways that comply with the requirements of this title. A preliminary analysis of these activities suggests that the federal cost will be on the order of $31 million. We are currently in the process of refining these estimates and will include better information on them in the final rule.

Costs to State Governments

The proposed rule will also have a cost effect on various state agencies that administer programs that require the use of individual health information. State agencies or programs clearly affected by the rule are those that meet the definition of a covered entity. The costs when government entities are serving as providers are included in the total cost estimates. However, non-covered agencies or programs that handle medical information, either under permissible exceptions to the disclosure rules or through an individual's expressed authorization, will likely incur some costs complying with provisions of this rule. Samples of state agencies encompassed by the broad scope of this rule include the: Medicaid, Children's Health Insurance program at the Department of Health and Human Services.

We have included state costs in the estimation of total costs. The greatest cost and administrative burden on the state government will fall to agencies and programs that act as covered entities, by virtue of being either a health plan or provider. Examples include the Medicaid, Children's Health Insurance program at the Department of Health and Human Services. These and other health insurance or provider programs operated by state government are subject to requirements placed on covered entities under this proposed rule, including, but not limited to, those outlined in Section D of the impact analysis. While many of these state programs already afford privacy protections for individual health information through the Privacy Act, this rule is expected to create additional requirements beyond those covered by existing Privacy Act rule. Further, we anticipate that most state health programs will, to some extent, need to modify their existing Privacy Act practices to fully comply with this rule.

The cost to state programs that function as health plans will be different than the private sector, much as the federal costs vary from private plans. A preliminary analysis suggests that state costs will be on the order of $90 million over five years. We will refine the estimates for the state government costs for enforcement, research and other distinct state government functions in the final rule. We welcome comment by state and local governments which will help the Department improve its analysis on these state costs.

F. Benefits

As we have discussed in the preamble, there are important societal benefits associated with improving health information privacy. Confidentiality is a key component of trust between patients and providers, and some studies indicate that a lack of privacy may deter patients from obtaining preventive care and treatment.[21] For these reasons, traditional approaches to estimating the value of a commodity cannot fully capture the value of personal privacy. It may be difficult for individuals to assign value to privacy protection because most individuals view personal privacy as a right. Because we promote the view that privacy protection is an important personal right, 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, suggest that the regulation is warranted. Added to these benefits is the intangible value of privacy, the personal security that we may feel when our records are confidential, which is very real and very significant but for which there is no economic value or proxy.

There are a number of ways to discuss the expected benefits of this proposed regulation. The first option is to discuss the benefits qualitatively. We believe that this is necessary to give the reader a basic understanding of how this proposed regulation will benefit society. The second option that we have used is to quantify the benefits of the proposed rule as they would apply to a few illness categories that may be particularly responsive to privacy concerns. This quantitative discussion is meant to be illustrative of the benefits rather than a comprehensive accounting of all of the benefits of the proposed rule. The combination of the two approaches clearly illustrates that the benefits of the regulation are significant in relation to the economic costs.

Before beginning our discussion of the benefits, it is important to create a framework for how the costs and benefits may be viewed in terms of individuals rather than societal aggregates. We have estimated the value an insured individual would need to place on increased privacy to make the proposed Privacy regulation a net benefit to those who receive health insurance. Our estimates are derived from data produced by the 1998 Current Population Survey from the Census Bureau, and report that 220 million persons are covered by either private or public health insurance. Joining the Census Bureau data with cost assumptions calculated in Section E, we have estimated the cost of the proposed regulation is $3.41 per insured individual. If we assume that individuals who use the health care system will be willing to pay more than $3.41 per year (or approximately $0.28 per month) to improve health information privacy, the benefits of the proposed regulation will outweigh the cost.

This is a conservative estimate of the number of people who will benefit from the regulation because it assumes that only those individuals who have health insurance will use medical services or benefit from the provisions of the proposed regulation. Currently, there are 44 million Americans who do not have any form of health care insurance. In addition, the estimates do not include those who pay for medical care directly, without any insurance or government support. By lowering the number of users in the system, we have inflated our estimate of the per-person cost of the regulation, therefore, we assume that our estimate represents the highest cost to an individual.

An alternative approach to determining how people would have to value increased privacy for this regulation to be beneficial is to look at the costs divided by the number of encounters with health care professionals annually. Data from the Medical Expenditure Panel Survey (MEPS) produced by the Agency for Health Care Policy Research (AHCPR) report approximately 1.62 billion health care visits, or encounters annually (e.g., office visits, hospital and nursing home stays, etc.). As with our calculation of average annual cost per insured patient, we have divided the total cost of complying with the regulation ($751 million per year) by the total annual number of health care encounters. The cost of instituting requirements of the proposed regulation is $0.46 per health care encounter. If we assume that individuals would be willing to pay more than $0.46 per health care encounter to improve health information privacy, the benefits of the proposed regulation will outweigh the cost.

Qualitative Discussion

A well designed privacy standard can be expected to build confidence among the public about the confidentiality of their medical records. The seriousness of public concerns about privacy in general are shown in the 1994 Equifax-Harris Consumer Privacy Survey, where ''84 percent of Americans are either very or somewhat concerned about threats to their personal privacy.''[22] A 1999 report, ''Promoting Health and Protecting Privacy'' notes ''* * * many people fear their personal health information will be used against them: to deny insurance, employment, and housing, or to expose them to unwanted judgements and scrutiny.''[23] These concerns would be partly allayed by the privacy standard. Further, increased confidence will increase the likelihood of some people seeking treatment for particular classes of disease. It will also change the dynamic of current payments. Insured patients currently paying out-of-pocket for confidentiality reasons will be more likely to file with their insurer. The increased utilization that would result from increased confidence in privacy could be beneficial under many circumstances. For many medical conditions, early treatment can lead to lower costs.

Fear of disclosure of treatment is an impediment to health care for many Americans. In the 1993 Harris-Equifax Health Information Privacy Survey, 7 percent of respondents said they or a member of their immediate family had chosen not to seek medical services due to fear of harm to job prospects or other life opportunities. About 2 percent reported having chosen not to file an insurance claim because of concerns with privacy or confidentiality.[24] Increased confidence on the part of patients that their privacy would be protected would lead to increased

[21] Equifax-Harris Consumer Privacy Survey, 1994.

[22] *Consumer Privacy Survey*, Harris-Equifax, 1994, p. vi.

[23] *Promoting Health: Protecting Privacy*, California Health Care Foundation and Consumers Union, January 1999, p. 12.

[24] *Health Information Privacy Survey*, Harris-Equifax, 1993, pp. 49–50.

treatment among people who delay or never begin care, as well as among people who receive treatment but pay directly (to the extent that the ability to use their insurance benefits will reduce cost barriers to more complete treatment).

The following are four examples of areas where increased confidence in privacy would have significant benefits. They were chosen both because they are representative of widespread and serious health problems, and because they are areas where reliable and relatively complete data are available for this kind of analysis. The logic of the analysis, however, applies to any health condition. Even for relatively minor conditions, an individual still might be concerned with maintaining privacy, and even a person with no significant health problems is going to value privacy because of the possibility at some time they will have a condition that they want to keep private.

Cancer. The societal burden of disease imposed by cancer is indisputable. Cancer is the second leading cause of death in the US,[25] exceeded only by heart disease. In 1999, 1.38 million new cancer cases will be diagnosed, as well as 900,000 new basal and squamous skin cell cancers. [26] The National Cancer Institute estimates that the overall cost of cancer is $104 billion; $35 billion in direct medical cost, $12 billion for morbidity costs (cost of lost productivity) and $57 billion for mortality costs.[27]

Among the most important elements in the fight against cancer are screening, early detection and treatment of the disease. However, however, many patients are concerned that some screening procedures will make them vulnerable to discrimination by insurers or employers. These privacy concerns have been cited as a reason patients do not seek early treatment for diseases such as cancer. As a result of forgoing early screening, cancer patients may ultimately face a more severe illness. For example, half of new diagnoses occur among types of cancer for which screening is available. Based on this research, studies show that if Americans participated in regular cancer screening, the rate of survival among patients who have screening-accessible cancers could increase to 95 percent.[28]

Approximately 184,300 women will be diagnosed with breast cancer this year,[29] and 25,000 women will be diagnosed with ovarian cancer.[30] In the same year, almost 44,000 women will die of breast cancer,[31] and 14,500 will die from ovarian cancer.[32] Early detection of these cancers could have a significant impact on reducing loss due to disability and death. For example, only 24 percent of ovarian cancers are diagnosed in the early stages. Of these, approximately 90 percent of patients survive treatment. The survival rate of women who detect breast cancer early is similarly high; more than 90 percent of women who detect and treat breast cancer in its early stages will survive.[33]

Researchers have developed screening techniques to identify breast, ovarian, and colon cancers, and tests have been developed to identify the presence or absence of cellular abnormalities that may lead to cancer. Despite these technological advances, the principle of patient autonomy requires that patients must decide for themselves if they will submit to screening procedures. Many individuals fear that employers and insurers will use cancer screening to discriminate against them. Several studies illustrate that persons with and without cancer fear discrimination. Thus, despite the potential benefits that early identification of cancer may yield, many researchers find that patient concerns regarding the confidentiality of cancer screening may prevent them from requesting the test, and result in disability or loss of life.

HIV/AIDS. Early detection is essential for the health and survival of an HIV (Human Immunodeficiency Virus) positive person. Concerns about the confidentiality of HIV status may prevent some people from getting tested. For this reason, each state has passed some sort of legislation regarding the confidentiality of HIV status. However, HIV status can be revealed indirectly through disclosure of HAART (Highly Active Anti-Retroviral Therapy) or similar HIV treatment drug use. In addition, since HIV/AIDS (Acquired Immune Deficiency Syndrome) is often the only specially protected condition, ''blacked out'' information on medical charts could indicate HIV positive status.[34] Strengthening privacy protections beyond this disease could increase confidence in privacy regarding HIV as well. Drug therapy for HIV positive persons has proven to be a life-extending, cost-effective tool. [35] A 1998 study showed that beginning treatment with HAART in the early asymptomatic stage is more cost-effective than beginning it late. After five years, only 15 percent of patients with early treatment are estimated to develop an ADE (AIDS-defining event), whereas 29 percent would if treatment began later. Early treatment with HAART prolongs survival (adjusted for quality of life) by 6.2 percent. The overall cost-effectiveness of early HAART treatment is estimated at $23,700 per quality-adjusted year of life saved.[36]

Other Sexually Transmitted Diseases. It is difficult to know how many people are avoiding testing for STDs despite having a sexually transmitted disease. A 1998 study by the Kaiser Family Foundation found that the incidence of disease was 15.3 million in 1996, though there is great uncertainty due to under-reporting.[37] For a potentially embarrassing disease such as an STD, seeking treatment requires trust in both the provider and the health care system for confidentiality. Greater trust should lead to more testing and greater levels of treatment. Earlier treatment for curable STDs can mean a decrease in morbidity and the costs associated with complications. These include expensive fertility problems, fetal blindness, ectopic pregnancies, and other reproductive complications.[38] In addition, there could be greater overall savings if earlier treatment translates into reduced spread of infections.

Substance Abuse and Mental Health Treatment. When individuals have a better understanding of the privacy practices that we are requiring in this proposed rule, some will be less reluctant to seek substance abuse and mental health treatment. One way that individuals will receive this information is through the notice requirement.

---

[25] American Cancer Society. http://4a2z.com/cgi/rfr.cgi?4CANCER-2-http://www.cancer.org/frames.html

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

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

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

[29] Avon's Breast Cancer Crusade. http://www.pmedia.com/Avon/library/faq.html

[30] Ovarian Cancer National Alliance. http://www.ovariancancer.org/index.shtml

[31] Cancer Statistics, 1999, Landis, Murray, Bolden and Wingo. CA: A Cancer Journal for Clinicians, Jan/Feb, 1999, Vol. 49, No. 1

[32] Ovarian Cancer National Alliance. http://www.ovariancancer.org/index.shtml

[33] Breast Cancer Information Service. http://trfn.clpgh.org/bcis/FAQ/facts2.html

[34] *Promoting Health: Protecting Privacy,* California Health Care Foundation and Consumers Union, January 1999, p. 13.

[35] For example, Roger Detels, M.D., et al., in ''Effectiveness of Potent Anti-Retroviral Therapy * * * ''JAMA, 1998; 280: 1497–1503 note the impact of therapy on HIV persons with respect to lengthening the time to development of AIDS, not just delaying death in persons who already have AIDS.

[36] 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.

[37] *Sexually Transmitted Diseases in America,* Kaiser Family Foundation, 1998. p. 12.

[38] Standard Medical information; see *http://www.mayohealth.org* for examples.

Increased use of mental health services would be expected to be beneficial to the persons receiving the care, to their families, and to society at large. The individual direct benefit from treatment would include an improved quality of life, reduced disability associated with the mental conditions, and a reduced mortality rate. The benefit to families would include quality of life improvements and reduced medical costs for other family members associated with abusive behavior by the treated individual. The benefit to society would include reduced costs of crime and reduced future public program treatment costs.

The 1998 Substance Abuse and Mental Health Statistics Source Book from SAMHSA reports cost-of-disease estimates from a range of studies, suggesting several hundred billion dollars of non-treatment costs associated with alcohol, drug, and mental (ADM) disorders. As an example of the magnitude of costs associated with mental health treatment, a 1997 National Institutes of Health report suggests that the total economic cost of mental health disorders such as anxiety, depressive (mood) disorders, eating disorders, and schizophrenia is approximately $115.5 billion annually.[39] Evidence suggests that appropriate treatment of mental health disorders can result in 50–80 percent of individuals experiencing improvements in these types of conditions. Improvements in patient functioning and reduced hospital stays could result in hundreds of million of dollars in cost savings annually.

The potential additional economic benefits associated with improving patient confidentiality and thus encouraging some unknown portion of individuals to either seek initial mental health treatment or increase service use are difficult to quantify well. Nevertheless, one can lay out a range of possible benefit levels to illustrate the possibility of cost savings associated with an expansion of mental health treatment to individuals who, due to protections offered by the privacy regulation, might seek mental health treatment that they otherwise would not have absent this regulation. This can be illustrated by drawing upon existing data on both the economic costs of mental illness and the treatment effectiveness of mental health interventions.

Although figures on the number of individuals who avoid mental health treatment due to privacy concerns do not exist, some indirect evidence is available. A 1993 Harris-Equifax Health Information Privacy Survey (noted earlier) found that 7 percent of respondents reported that they or a member of their immediate family had chosen not to seek services for a physical or mental health condition due to fear of harm to job prospects or other life opportunities. It should be noted that this survey is somewhat dated and represents only one estimate. Moreover, given the wording of the question, there are other reasons aside from privacy concerns that led these individuals to respond positively.

For the purpose of an illustration, however, assumptions can be made about what proportion of the 7 percent responding affirmatively to this question may have avoided seeking mental health services due to privacy concerns. Given the proportion of mental health services that compromise total health care services in this country, a reasonable upper limit of the number of individuals avoiding mental health treatment due to privacy concerns might be 1.8 percent (*i.e.,* 25% of 7%), while a reasonable lower limit might be 0.36 percent (*i.e.,* 5% of 7%). Taking these figures as upper and lower limits, it is possible to estimate potential benefits by multiplying these figures by the annual economic cost reductions associated with treatment effectiveness rates. For example, using the upper limit of 1.8 percent, multiplying this by the annual economic costs of mental illness ($115.5 billion) and a treatment effectiveness rate of 80 percent, yields an estimate of potential annual benefits of $1,663,200,000. Similarly, using the upper limit of 1.8 percent coupled with a treatment effectiveness rate of 50 percent yields an estimate of potential annual benefits of $1,039,500,000. Assuming a lower limit of 0.36 percent more individuals seeking mental health treatment due to enhance privacy protections, coupled with a treatment effectiveness rate of 80% yields an estimate of potential annual benefits of $332,640,000. Similarly, using the lower limit of 0.36 percent coupled with a treatment effectiveness rate of 50 percent yields an estimate of potential annual benefits of $207,900,000. Therefore, given the existing data on the annual economic costs of mental illness and the rates of treatment effectiveness for these disorders, coupled with assumptions regarding the percentage of individuals who might seek mental health treatment under conditions of greater privacy protections, the potential additional economic benefit in this one treatment area could range from approximately $208 million to $1.67 billion annually.

TABLE 3.—POTENTIAL BENEFITS OF THE PROPOSED PRIVACY REGULATION FROM COST SAVINGS DUE TO EARLY TREATMENT OF MENTAL HEALTH DISORDERS

Illness	Total annual economic cost of illness (in billions)	Percent net cost reduction if additional care is received
Mental Health—Anxiety Disorders	$46.6	70–90
Mental Health—Depressive (Mood) Disorders	30.4	60–80
Mental Health—Eating Disorders	6.0	40–60
Mental Health—Schizophrenia	32.5	60–85
Total	115.5	N/A

[39] *Disease-Specific Estimates of Direct and Indirect Costs of Illness and NIH Support; 1997 Update,* 1997.

G. Examination of Alternative Approaches

1. Creation of De-identified Information (164.506(d))

We considered defining ''individually identifiable health information'' as any information that is not anonymous, that is, for which there is any possibility of identifying the subject. We rejected this option, for several reasons. First, the statute suggests a different approach. The term ''individually identifiable health information'' is defined in HIPAA as health information that:

> * * * identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

By including the modifier ''reasonable basis,'' Congress appears to reject the absolute approach to defining ''identifiable.'' Covered entities would not always have the statistical sophistication to know with certainty when sufficient identifying information has been removed so that the record is no longer identifiable. We believe that covered entities need more concrete guidance as to when information will and will not be ''identifiable'' for purposes of this regulation.

Defining non-identifiable to mean anonymous would require covered entities to comply with the terms of this regulation with respect to information for which the probability of identification of the subject is very low. We want to encourage covered entities and others to remove obvious identifiers or encrypt them whenever possible; use of the absolute definition of ''identifiable'' would not promote this salutary result.

For these reasons, we propose at § 164.506(d)(2)(ii) that there be a presumption that, if specified identifying information is removed and if the holder has no reason to believe that the remaining information can be used by the reasonably anticipated recipients alone or in combination with other information to identify an individual, then the covered entity would be presumed to have created de-identified information.

At the same time, in proposed § 164.506(d)(2)(iii), we are leaving leeway for more sophisticated data users to take a different approach. We are including a ''reasonableness'' standard so that entities with sufficient statistical experience and expertise could remove or code a different combination of information, so long as the result is still a low probability of identification. With this approach, our intent is to provide certainty for most covered entities, while not limiting the options of more sophisticated data users.

In this rule we are proposing that covered entities and their business partners be permitted to use protected health information to create de-identified health information. Covered entities would be permitted to further use and disclose such de-identified information in any way, provided that they do not disclose the key or other mechanism that would enable the information to be re-identified, and provided that they reasonably believe that such use or disclosure of de-identified information will not result in the use or disclosure of protected health information. See proposed § 164.506(d)(1). This means that a covered entity could not disclose de-identified information to a person if the covered entity reasonably believes that the person would be able to re-identify some or all of that information, unless disclosure of protected health information to such person would be permitted under this proposed rule. In addition, a covered entity could not use or disclose the key to coded identifiers if this rule would not permit the use or disclosure of the identified information to which the key pertains. If a covered entity re-identifies the de-identified information, it may only use or disclose the re-identified information consistent with these proposed rules, as if it were the original protected health information.

We invite comment on the approach that we are proposing and on whether alternative approaches to standards for entities determining when health information can reasonably be considered no longer individually identifiable should be considered.

2. General Rules (§ 164.506)

As a general rule, we are proposing that protected health information not be used or disclosed by covered entities except as authorized by the individual who is the subject of such information or as explicitly provided this rule. Under this proposal, most uses and disclosures of an individual's protected health information would not require explicit authorization by the individual, but would be restricted by the provisions of the rule. Covered entities would be able to use or disclose an individual's protected health information without authorization for treatment, payment and health care operations. See proposed § 164.506(a)(1)(i). Covered entities also would be permitted to use or disclose an individual's protected health information for specified public and public policy-related purposes, including public health, research, health oversight, law enforcement, and use by coroners. Covered entities would be *permitted* by this rule to use and disclose protected health information when required to do so by other law, such as a mandatory reporting requirement under State law or pursuant to a search warrant. See proposed § 164.510. Covered entities would be *required* by this rule to disclose protected health information for only two purposes: to permit individuals to inspect and copy protected health information about them (see proposed § 164.514) and for enforcement of this rule (see proposed § 164.522(d)).

Covered entities of all types and sizes would be required to comply with the proposed privacy standards outlined below. The proposed standards would not impose particular mechanisms or procedures that covered entities must adopt to implement the standards. Instead, we would require that each affected entity assess its own needs and devise, implement, and maintain appropriate privacy policies, procedures, and documentation to address its business requirements. How each privacy standard would be satisfied would be a business decision that each entity would have to make. This permits the privacy standards to establish a stable baseline, yet remain flexible enough to take advantage of developments and methods for protecting privacy that will evolve over time.

Because the privacy standards would need to be implemented by all covered entities, from the smallest provider to the largest, multi-state health plan, a single approach to implementing these standards would be neither economically feasible nor effective in safeguarding health information privacy. For example, in a small physician practice the office manager might be designated to serve as the privacy official as one of many duties (see proposed § 164.518(a)) whereas at a large health plan, the privacy official may constitute a full time position and have the regular support and advice of a privacy staff or board.

In taking this approach, we intend to strike a balance between the need to maintain the confidentiality of protected health information and the economic cost of doing so. Health care entities must consider both aspects in devising their solutions. This approach is similar to the approach we proposed in the Notice of Proposed Rulemaking for the administrative simplification security and electronic signature standards.

3. Use and Disclosure for Treatment, Payment, and Health Care Operations (§ 164.506(a))

We are proposing that, subject to limited exceptions for psychotherapy notes and research information unrelated to treatment discussed below, a covered entity be permitted to use or disclose protected health information without individual authorization for treatment, payment or health care operations.

We are not proposing to require individual authorizations of uses and disclosures for health care and related purposes, although such authorizations are routinely gathered today as a condition of obtaining health care or enrolling in a health plan. Although many current disclosures of health information are made pursuant to individual authorizations, these authorizations provide individuals with little actual control over their health information. When an individual is required to sign a blanket authorization at the point of receiving care or enrolling for coverage, that consent is often not voluntary because the individual must sign the form as a condition of treatment or payment for treatment. Individuals are also often asked to sign broad authorizations but are provided little or no information about how their health information would be or will in fact be used. Individuals cannot make a truly informed decision without knowing all the possible uses, disclosures and re-disclosures to which their information will be subject. In addition, since the authorization usually precedes creation of the record, the individual cannot predict all the information the record could contain and therefore cannot make an informed decision as to what would be released.

Our proposal is intended to make the exchange of protected health information relatively easy for health care purposes and more difficult for purposes other than health care. For individuals, health care treatment and payment are the core functions of the health care system. This is what they expect their health information will be used for when they seek medical care and present their proof of insurance to the provider. Consistent with this expectation, we considered requiring a separate individual authorization for every use or disclosure of information but rejected such an approach because it would not be realistic in an increasingly integrated health care system. For example, a requirement for separate patient authorization for each routine referral could impair care, by delaying consultation and referral as well as payment.

We therefore propose that covered entities be permitted to use and disclose protected health information without individual authorization for treatment and payment purposes, and for related purposes that we have defined as health care operations. For example, providers could maintain and refer to a medical record, disclose information to other providers or persons as necessary for consultation about diagnosis or treatment, and disclose information as part of referrals to other providers. Providers also could use a patient's protected health information for payment purposes such as submitting a claim to a payer. In addition, providers could use a patient's protected health information for health care operations, such as use for an internal quality oversight review. We would note that, in the case of an individual where the provider has agreed to restrictions on use or disclosure of the patient's protected health information, the provider would be bound by such restrictions as provided in § 164.506(c).

We also propose to prohibit covered entities from seeking individual authorization for uses and disclosures for treatment, payment and health care operations unless required by State or other applicable law. As discussed above in section II.C, such authorizations could not provide meaningful privacy protections or individual control and could in fact cultivate in individuals erroneous understandings of their rights and protections.

The general approach that we are proposing is not new. Some existing State health confidentiality laws permit disclosures without individual authorization to other health care providers treating the individual, and the Uniform Health-Care Information Act permits disclosure ''to a person who is providing health-care to the patient'' (9 Part I, U.L.A. 475, 2–104 (1988 and Supp. 1998)). We believe that this approach would be the most realistic way to protect individual confidentiality in an increasingly data-driven, electronic and integrated health care system. We recognize, however, that particularly given the limited scope of the authority that we have under this proposed rule to reach some significant actors in the health care system, that other approaches could be of interest. We invite comments on whether other approaches to protecting individuals' health information would be more effective.

4. Minimum Necessary Use and Disclosure (§ 164.506(b))

We propose that, except as discussed below, a covered entity must make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose of the use or disclosure, taking into consideration technological limitations.

Under this proposal, covered entities generally would be required to establish policies and procedures to limit the amount of protected health care information used or disclosed to the minimum amount necessary to meet the purpose of the use or disclosure, and to limit access to protected health information only to those people who need access to the information to accomplish the use or disclosure. With respect to use, if an entity consists of several different components, the entity would be required to create barriers between components so that information is not used inappropriately. The same principle applies to disclosures.

A ''minimum necessary'' determination would need to be consistent with and directly related to the purpose of the use or disclosure and take into consideration the ability of a covered entity to delimit the amount of information used or disclosed and the relative burden imposed on the entity. The proposed minimum necessary requirement is based on a reasonableness standard: covered entities would be required to make reasonable efforts and to incur reasonable expense to limit the use and disclosure of protected health information as provided in this section.

In our discussions of the minimum necessary requirement, we considered whether or not this should apply to all entities and whether or not it should be applied to all protected health information. We decided that the principle of minimum necessary disclosure is critical to the protection of privacy and that because small entities represent 83 percent of the health care industry, we would not exempt them from this provision without undermining its effectiveness.

We understand that the requirements outlined in this section do not create a bright line test for determining the minimum necessary amount of protected health information appropriate for most uses or disclosures. Because of this lack of precision, we considered eliminating the requirement altogether. We also considered merely requiring covered entities to address the concept within their internal privacy procedures, with no further guidance as to how each covered entity would address the issue. These approaches were rejected because minimizing both the amount of protected health information used and disclosed within the health care system and the number of persons who have access to such information is vital if we are to successfully enhance the confidentiality of people's personal health information. We invite comments on the approach that we have adopted and on alternative methods of implementing the minimum necessary principle.

5. Right To Restrict Uses and Disclosures (§ 164.506(c))

We propose to permit in § 164.506(c) that individuals be able to request that a covered entity restrict further uses and disclosures of protected health information for treatment, payment, or health care operations, and if the covered entity agrees to the requested restrictions, the covered entity could not make uses or disclosures for treatment, payment or health care operations that are inconsistent with such restrictions, unless such uses or disclosures are mandated by law. This provision would not apply to health care provided to an individual on an emergency basis.

We should note that there is nothing in this proposed rule that would require a covered entity to agree to a request to restrict, or to treat or provide coverage to an individual requesting a restriction under this provision. Covered entities who do not wish to, or due to contractual obligations cannot, restrict further use or disclosure are not obligated to agree to a request under this provision.

We considered providing individuals substantially more control over their protected health information by requiring all covered entities to attempt to accommodate any restrictions on use and disclosure requested by patients. We rejected this option as unworkable. While industry groups have developed principles for requiring patient authorizations, we have not found widely accepted standards for implementing patient restrictions on uses or disclosures. Restrictions on information use or disclosure contained in patient consent forms are sometimes ignored because they may not be read or are lost in files. Thus, it seems unlikely that a requested restriction could successfully follow a patient's information through the health care system—from treatment to payment, through numerous operations, and potentially through certain permissible disclosures. Instead we would limit the provision to restrictions that have been agreed to by the covered entity.

We recognize that the approach that we are proposing could be difficult because of the systems limitations described above. However, we believe that the limited right for patients proposed in this proposed rule can be implemented because it only applies in instances in which the covered entity agrees to the restrictions. We assume that covered entities would not agree to restrictions that they are unable to implement.

We considered limiting the rights under this provision to patients who pay for their own health care (or for whom no payment was made by a health plan). Individuals and providers that engage in self-pay transactions have minimal effect on the rights or responsibilities or payers or other providers, and so there would be few instances when a restriction agreed to in such a situation would have negative implications for the interests of other health care actors. Limiting the right to restrict to self-pay patients also would reduce the number of requests that would be made under this provision. We rejected this approach, however, because the desire to restrict further uses and disclosures arises in many instances other than self-pay situations. For example, a patient could not want his or her records shared with a particular physician because that physician is a family friend. Or an individual could be seeking a second opinion and may not want his or her treating physician consulted. Individuals have a legitimate interest in restricting disclosures in these situations. We solicit comment on the appropriateness of limiting this provision to instances in which no health plan payment is made on behalf of the individual.

6. Application to Business Partners (§ 164.506(e))

In § 164.506(e), we propose to require covered entities to take specific steps to ensure that protected health information disclosed to a business partner remains protected. We intend these provisions to allow customary business relationships in the health care industry to continue while providing privacy protections to the information shared in these relationships. Business partners would not be permitted to use or disclose protected health information in ways that would not be permitted of the covered entity itself under these rules.

Other than for purposes of consultation or referral for treatment, we would allow covered entities to disclose protected health information to business partners only pursuant to a written contract that would, among other specified provisions, limit the business partner's uses and disclosures of protected health information to those permitted by the contract, and would impose certain security, inspection and reporting requirements on the business partner. We would hold the covered entity responsible for certain violations of this proposed rule made by their business partners, and require assignment of responsibilities when a covered entity acts as a business partner of another covered entity.

Under this proposed rule, a business partner would be acting on behalf of a covered entity, and we propose that its use or disclosure of protected health information be limited to the same extent that the covered entity for whom they are acting would be limited. Thus, a business partner could have no more authority to use or disclose protected health information than that possessed by the covered entity from which the business partner received the information. We would note that a business partner's authority to use and disclose protected health information could be further restricted by its contract with a covered entity, as described below.

We are not proposing to require the business partners of covered entities to develop and distribute a notice of information practices, as provided in proposed § 164.512. A business partner would, however, be bound by the terms of the notice of the covered entity from which it obtains protected health information. See proposed § 164.506(e). We are proposing this approach so that individuals could rely on the notices that they receive from the covered entities to which they disclose protected health information. If the business partners of a covered entity were able to make wider use or make more disclosures than the covered entity, the patients or enrollees of the covered entity would have difficulty knowing how their information was being used and to whom it was being disclosed.

We are also proposing that a business partner's use and disclosure of protected health information be limited by the terms of the business partner's contractual agreement with the covered entity. We propose that a contract between a covered entity and a business partner could not grant the business partner authority to make uses or disclosures of protected health information that the covered entity itself would not have the authority to make. The contract between a covered entity and a business partner could further limit the business partner's authority to use or disclose protected health information as agreed to by the parties. Further, the business partner would have to apply the same limitations to its subcontractors (or persons with similar arrangements) who assist with or carry out the business partner's activities.

To help ensure that the uses and disclosures of business partners are limited to those recognized as appropriate by the covered entities from whom they receive protected health information, subject to the exception discussed below, we are proposing that covered entities be prohibited from disclosing protected health information to a business partner unless the covered entity has entered into a written contract with the business partner that meets the requirements of this subsection. See proposed § 164.506(e)(2)(i).

The contract requirement that we are proposing would permit covered entities to exercise control over their business partners' activities and provides documentation of the relationship between the parties, particularly the scope of the uses and disclosures of protected health information that business partners could make. The presence of a contract also would formalize the relationship, better assuring that key questions such as security, scope of use and disclosure, and access by subject individuals are adequately addressed and that the roles of the respective parties are clarified. Finally, a contract can bind the business partner to return any protected health information from the covered entity when the relationship is terminated.

In lieu of a contracting requirement, we considered imposing only affirmative duties on covered entities to ensure that their relationships with business partners conformed to the standards discussed in the previous paragraph. Such an approach could be considered less burdensome and restrictive, because we would be leaving it to the parties to determine how to make the standards effective. We rejected this approach primarily because we believe that in the vast majority of cases, the only way that the parties could establish a relationship with these terms would be through contract. We also determined that the value of making the terms explicit through a written contract would better enable the parties to know their roles and responsibilities, as well as better enable the Secretary to exercise her oversight role. In addition, we understand that most covered entities already enter into contracts in these situations and therefore this proposal would not disturb general business practice. We invite comment on whether there are other contractual or non-contractual approaches that would afford an adequate level of protection to individuals' protected health information. We also invite comment on the specific provisions and terms of the proposed approach.

We are proposing one exception to the contracting requirement: when a covered entity consults with or makes a referral to another covered entity for the treatment of an individual, we would propose that the sharing of protected health information pursuant to that consultation or referral not be subject to the contracting requirement described above. See proposed § 164.506(e)(1)(i). Unlike most business partner relationships, which involve the systematic sharing of protected health information under a business relationship, consultation and referrals for treatment occur on a more informal basis among peers, and are specific to a particular individual. Such exchanges of information for treatment also appear to be less likely to raise concerns about further impermissible use or disclosure, because providers receiving such information are unlikely to have a commercial or other interest in using or disclosing the information. We invite comment on the appropriateness of this exception, and whether there are additional exceptions that should be included in the final regulation.

We note that covered health care providers receiving protected health information for consultation or referral purposes would still be subject to this rule, and could not use or disclose such protected health information for a purpose other than the purpose for which it was received (i.e., the consultation or referral). Further, we note that providers making disclosures for consultations or referrals should be careful to inform the receiving provider of any special limitations or conditions to which the disclosing provider has agreed to impose (e.g., the disclosing provider has provided notice to its patients that it will not make disclosures for research).

We are proposing that covered entities be accountable for the uses and disclosures of protected health information by their business partners. A covered entity would be in violation of this rule if the covered entity knew or reasonably should have known of a material breach of the contract by a business partner and it failed to take reasonable steps to cure the breach or terminate the contract. See proposed § 164.506(e)(2)(iii). A covered entity that is aware of impermissible uses and disclosures by a business partner would be responsible for taking such steps as are necessary to prevent further improper use or disclosures and, to the extent practicable, for mitigating any harm caused by such violations. This would include, for example, requiring the business partner to retrieve inappropriately disclosed information (even if the business partner must pay for it) as a condition of continuing to do business with the covered entity. A covered entity that knows or should know of impermissible use of protected health information by its business partner and fails to take reasonable steps to end the breach would be in violation of this rule.

We considered requiring covered entities to terminate relationships with business partners if the business partner committed a serious breach of contact terms required by this subpart or if the business partner exhibited a pattern or practice of behavior that resulted in repeated breaches of such terms. We rejected that approach because of the substantial disruptions in business relationships and customer service when terminations occur. We instead require the covered entity to take reasonable steps to end the breach and mitigate its effects. We would expect covered entities to terminate the arrangement if it becomes clear that a business partner cannot be relied upon to maintain the privacy of protected health information provided to it. We invite comments on our approach here and whether requiring automatic termination of business partner contracts would be warranted in any circumstances.

We also considered imposing more strict liability on covered entities for the actions of their business partners, just as principals are strictly liable for the actions of their agents under common law. We decided, however, that this could impose too great a burden on covered entities, particularly small providers. We are aware that, in some cases, the business partner will be larger and more sophisticated with respect to information handling than the covered entity. Therefore we instead opted to propose that covered entities monitor use of protected health information by business partners, and be held responsible only when they knew or should have known of improper use of protected health information.

Our intention in this section is to recognize the myriad of business relationships that currently exist and to ensure that when they involve the exchange of protected health information, the roles and responsibilities of the different parties with respect to the protected health information are clear. We do not propose to fundamentally alter the types of business relationships that exist in the health care industry or the manner in which they function. We request comments on the extent to which our proposal would disturb existing contractual or other arrangements among covered entities and business partners.

7. Application to Information About Deceased Persons (§ 164.506(f))

We are proposing that information otherwise protected by these regulations retain that protection for two years after the death of the subject of the information. The only exception that we are proposing is for uses and disclosures for research purposes.

HIPAA includes no temporal limitations on the application of the privacy protections. Although we have the authority to protect individually identifiable health information maintained by a covered entity indefinitely, we are proposing that the requirements of this rule generally apply for only a limited period, as discussed below. In traditional privacy law, privacy interests, in the sense of the right to control use or disclosure of information about oneself, cease at death. However, good arguments exist in favor both of protecting and not protecting information about the deceased. Considering that one of the underlying purposes of health information confidentiality is to encourage a person seeking treatment to be frank in the interest of obtaining care, there is good reason for protecting information even after death. Federal agencies and others sometimes withhold sensitive information, such as health information, to protect the privacy of surviving family members. At the same time, perpetual confidentiality has serious drawbacks. If information is needed for legitimate purposes, the consent of a living person legally authorized to grant such consent must be obtained, and the further from the date of death, the more difficult it may be to identify the person. The administrative burden of perpetual protection may eventually outweigh the privacy interests served.

While various State laws have been passed specifically addressing privacy of genetic information, there is currently no federal legislation that deals with these issues. We considered extending the two-year period for genetic and hereditary information, but were unable to construct criteria for protecting the possible privacy interests of living children without creating extensive burden for information holders and hampering health research. We invite comments on whether further action is needed in this area and what types of practical provisions may be appropriate to protect genetic and hereditary health information.

8. Uses and Disclosures With Individual Authorization (§ 164.508)

Covered entities would be required to obtain individual authorization to use individually identifiable health information for purposes other than those allowed under the rule. Activities requiring authorization include, for example, marketing. Costs will be ongoing for staffing and administrative activities related to obtaining authorization from individuals.

Our proposal is based on the precept that a combination of strict limits on how covered entities can use and disclose protected health information, adequate notice to individuals about how their information will be used, and guaranteeing individuals' rights to inspect, copy and amend their health records will provide patients with better privacy protection and more effective control over their information than alternative approaches to privacy protection.

This section addresses the requirements that we are proposing when protected health information is disclosed pursuant to the individual's explicit authorization. The regulation would require that covered entities have authorization from individuals before using or disclosing their protected health information for any purpose not otherwise recognized by this regulation. Circumstances where an individual's protected health information could be used or disclosed without authorization are discussed in connection with proposed §§ 164.510 and 164.522 below.

This section proposes different conditions governing such authorizations in two situations in which individuals commonly authorize covered entities to disclose information:

- Where the individual initiates the authorization because he or she wants a covered entity to disclose his or her record, and
- Where a covered entity asks an individual to authorize it to disclose or use information for purposes other than treatment, payment or health care operations.

The requirements proposed in this section are not intended to interfere with normal uses and disclosures of information in the health care delivery or payment process, but only to allow control of uses extraneous to health care. The restrictions on disclosure that the regulation would apply to covered entities may mean that some existing uses and disclosures of information could take place only if the individual explicitly authorized them under this section.

We considered requiring a uniform set of requirements for all authorizations, but concluded that it would be appropriate to treat authorizations initiated by the individual differently from authorizations sought by covered entities. There are fundamental differences, in the uses of information and in the relationships and understandings among the parties, in these two situations. When individuals initiate authorizations, they are more likely to understand the purpose of the release and to benefit themselves from the use or disclosure. When a covered entity asks the individual to authorize disclosure, we believe the entity should make clear what the information will be used for, what the individual's rights are, and how the covered entity would benefit from the requested disclosure.

We are proposing several requirements that would have to be met in the authorization process when the individual has initiated the authorization. We understand that the requirements that we are imposing here would make it quite unlikely that an individual could actually initiate a completed authorization, because few individuals would know to include all of these elements in a request for information. In most instances, individuals authorize a use or disclosure by completing a form provided by a third party, either the ultimate recipient of the information (who may have a form authorizing them to obtain the records from the record holders) or a health care provider or health plan holding the records (who may have a form that documents a request for the release of records to a third party). For this reason, we do not believe that our proposal would create substantial new burdens on individuals or covered entities in cases when an individual is initiating an authorized release of information. We invite comment on whether we are placing new burdens on individuals or covered entities. We also invite comment on whether the approach that we have proposed provides sufficient protection to individuals who seek to have their protected health information used or disclosed.

We are proposing that when covered entities initiate the authorization by asking individuals to authorize disclosure, the authorization be required to include all of the items required above as well as several additional items. We are proposing additional requirements when covered entities initiate the request for authorization, because in many cases it could be the covered entity, and not the individual, that achieves the primary benefit of the disclosure. We considered permitting covered entities to request authorizations with only the basic features proposed for authorizations initiated by the individual, for the sake of simplicity and consistency. However, we believe that additional protections are merited when the entity that provides or pays for health care requests authorizations to avert possible coercion.

We also acknowledge that there will be costs related to moving away from a blanket authorization system. These costs will be discussed more explicitly in the sections on allowable disclosures (both with and without authorization).

Covered entities and third parties that wish to have information disclosed to them will prepare forms for individuals to use to authorize use or disclosure. A model authorization form is displayed in Appendix A to this proposed rule. We considered presenting separate model forms for the two different types of authorizations (initiated by the individual and not initiated by the individual). However, this approach could be subject to misuse and be confusing to covered entities and individuals, who may be unclear as to which form is appropriate in specific situations. The model in the appendix accordingly is a unitary model, which includes all of the requirements for both types of authorization. By following such a model, covered entities, particularly small entities, could avoid the legal and administrative expenses that would be necessary to develop an authorization form that complies with the rule's requirements. The proposed rule does not prevent entities from developing or modifying their own authorization forms. The alternative to providing this model was to simply state that an authorization would be required and allow entities to develop the authorization independently. While we would specify some information required in the authorization in this alternative, we would not give an actual form. This was considered to be an unnecessary burden for entities.

Finally, we are proposing that an individual be permitted to revoke an authorization at any time except to the extent that action has been taken in reliance on the authorization. See proposed § 164.508(e).

9. Uses and Disclosures Permitted Without Individual Authorization (§ 164.510)

This section describes uses and disclosures of protected health information that covered entities could make for purposes other than treatment, payment, and health care operations without individual authorization, and the conditions under which such uses and disclosures could be made. We propose to allow covered entities to use or disclose protected health information without individual authorization for such purposes if the use or disclosure would comply with the applicable requirements of this section.

Covered entities could need to reevaluate and modify their operating procedures to comply with the proposed rule's prohibition on disclosing individually identifiable health information without patient authorization for any purpose other than treatment, payment, health care operations, or those situations explicitly identified as permissible disclosures under this proposed rule. Many entities could already do this. Entities that do not do this would need to alter information management systems and implement administrative policies and procedures to prevent inappropriate disclosures. Entities would also have to determine whether or not an authorization is necessary for each disclosure beyond treatment, payment, and health care operations that is not explicitly defined as a permissible disclosure under this proposed rule. It should be noted that the minimum necessary principle is an important component of the costs related to any disclosure. We expect that there would be significant initial and ongoing costs.

If an entity chooses to disclose protected health information without authorization from individuals, there would be a number of new provisions that it would have to comply with. For example, if a disclosure is to researchers outside of the organization, the entity must obtain written documentation indicating that the research has been approved by an institutional review board (IRB) or equivalent process by a privacy board. This requirement is associated with ongoing administrative costs. We note that any such costs are optional unless other requirements (state laws, mandatory reporting systems, etc.) mandate these disclosures. In order to minimize the burden of these costs for mandatory disclosures, we have tried to apply as few business partner requirements as possible in areas where these mandatory disclosures are possible. However, in cases where the disclosure is optional, entities would have higher costs if they choose to use these disclosures. We expect that entities would consider these costs before making any such disclosure and determine if the benefits to their business of disclosure are greater than the costs related to making the disclosure. Additionally, other than the new requirements for disclosures for research, most of the disclosures are simply recognizing current practices and would not require large new costs.

We considered permitting uses and disclosures only where law affirmatively requires the covered entity to use or disclose protected health information. However, because the activities described below are so important to the population as a whole, we decided to permit a covered entity to use or disclose information to promote those activities even when such activities are not legally mandated. In some cases, however, we would permit a use or disclosure only when such use or disclosure is authorized by other law. The requirements for verification of legal authority are discussed in section II.G.3.

Disclosures that are required by current law would only require minimal additional costs to entities. The only cost directly attributable to this proposed requirement would be the additional cost of noting these disclosures on the accounting of uses and disclosures.

However, disclosures required by this proposed regulation should be considered new costs. These mandatory disclosures would be extremely rare. For example, we expect that the Department would limit the number of compliance audits conducted. In these cases, some of the more expensive activities, including the minimum necessary principle and determining whether or not to make the disclosure, would not be applicable.

We would restrict the discussion of discretionary disclosures to the general principles behind such disclosures rather than a detailed description of each allowable disclosure. More elaborate discussion of options for individual classes of disclosures can be found in the preamble. These disclosures are optional disclosures and therefore, any costs related to making these disclosures would incur optional costs. We do not have a complete understanding of how often these disclosures are currently made, nor do we understand what procedures are currently in place. We also do not understand how often these disclosures would be made given the new costs associated with such disclosures. Note that the degree of new costs imposed if an entity opts to use a disclosure varies dramatically depending on the type of disclosure. For example, a disclosure of directory information in a hospital would probably not involve significant additional costs, while research that is not subject to the common could would have significant new costs involved. These disclosures, and thus these costs, are optional under this proposed rule. While they may be mandated under other law, such mandated disclosures are already being made, so there would be no additional costs. In this case there are only marginal new costs related to these disclosures.

10. Clearinghouses and the Rights of Individuals

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 would include specific provisions regarding inspection, copying, amendment and correction. Therefore, we do not believe that 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 would 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.

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

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.

The rule requires covered entities to prepare and make available a notice that informs patients about their privacy rights and the entity’s actions to protect privacy. Entities that do not already comply with the rule’s requirements would incur one-time legal and administrative costs in preparing and making the notice available. In addition, plans would incur ongoing costs related to the dissemination of the notice at least once every three years, and all covered entities would have ongoing costs related to preparation of new notices as disclosure practices change, dissemination to new individuals who receive services, and requests for copies of the notice. Entities would also incur ongoing costs related to answering questions stemming from the notice. In addition to requiring a basic notice, we considered requiring a longer more detailed notice, that would be available to individuals on request. However, we decided that making information available on request, and letting the covered entity decide how best to provide such information, is a more balanced approach. We felt that it would be overly burdensome to all entities, especially small entities, to require two notices.

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 acknowledge 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.

We believe that the proposed rule appropriately balances a patient’s need for information and assurances regarding privacy with the covered entities’ need for flexibility in describing their operations and procedures to protect patient privacy. Instead of a model notice, we have included a sample notice to guide the development of notices. We felt that this would be an appropriate way to reduce the burden on all entities including those classified as small.

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 at Appendix A of this preamble.

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 to 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 would 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 would 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.

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.7, covered plans and providers may only use and disclose protected health information for purposes stated in this notice.

We considered requiring the notice to include not only a discussion of 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.

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.

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 on 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.

We propose 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 propose 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 providers to mail or otherwise disseminate their notices after giving the notice to individuals at the time of the first service delivery. 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 would 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.

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 providers consistent with giving individuals a clear source of accurate information.

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

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.

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.

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.

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.

We considered whether entities should be permitted to deny access to information based on a number of factors. For more specific discussion of access denials, please refer to earlier preamble text. For the purposes of the economic impacts, it is important to note that these denials are optional and, therefore, any costs associated with utilizing these denials are optional.

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 would 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.

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 could 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.

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 would 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 could arise where an individual would 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 could 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 could 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.

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.

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.

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).

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

In this proposed 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 would 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.

This proposed rule would 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 would permit them to respond to requests within the 30-day time period in this proposed rule.

We also considered whether or not the disclosure history should be a formal document that is constantly maintained or whether we should give more flexibility to entities in this regard. We decided that since our ultimate goal is that individuals have access to a disclosure history of their records upon request, it would be reasonable to require only that they be able to do this. We are not prescribing how they fulfill the requirement. We also believe that it is less burdensome to require that they be able to create a disclosure history than to require that they have a specific format for maintaining a disclosure history.

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 would be 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 entity 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.

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

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.

We are concerned about the burden that requests for amendment or correction could 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 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 the discussion in section II.F.4. We are soliciting comments whether this approach would effectively ensure that amendments and corrections are communicated appropriately.

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.

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 could 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.

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 could expect a final decision.

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 could 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 would do so, then it would not be reasonable for the covered plan or provider to incur the time and expense of notification. If, however, if 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.

We discussed a number of options regarding the notification of other entities. We considered only requiring that the entity provide the individual with a listing of who else could have received the information. This would place the burden of notification in the hands of the individual rather than the entity. Because individuals would not have the same contacts and relationship with other entities as the original covered entity, we decided that placing the burden on individuals would be more cumbersome for both individuals and the secondary entities receiving the requests. We also considered not including a notification requirement. However, this would mean that individuals would need to both figure out where the information had gone to and make separate requests for amendment or correction to every entity. This also appeared to be overly difficult. We believe that the option we are proposing is fair to both individuals and covered entities.

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.

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.

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.

15. Administrative Requirements (§ 164.518)

We propose that covered entities be required to implement five basic administrative requirements to safeguard protected health information: Designation of a privacy official, the provision of privacy training, establishment of safeguards, a complaint process, and establishment of sanctions. Implementation of these requirements would vary depending on a variety of different factors such as type of entity (e.g., provider or plan), size of entity (e.g., number of employees, number of patients), the level of automation within the entity (e.g., electronic medical records), and organization of the entity (e.g., existence of an office of information systems, affiliation with a medical school).

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

In proposed § 164.518(a), 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.

b. Training (§ 164.518(b))

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 all 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 would 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 would 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.

c. Safeguards (§ 164.518(c))

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.

i. *Verification procedures.*

As noted in section II.E., 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.

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.

d. 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. 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 proposed § 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.

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 could 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 could file a complaint with the Secretary before, during, after, or concurrent with filing a complaint 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 could be necessary to address the handling of classified information and solicit comment on the issue.

e. Sanctions (§ 164.518(e))

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 would 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.

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.

f. Sanctions (§ 164.518(f))

We propose in § 164.518(f) 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.

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

In proposed § 164.520, we would require covered entities to develop and document their policies and procedures for implementing the requirements of this proposed rule. This requirement is intended as a tool to facilitate covered entities' efforts to develop appropriate policies to implement this proposed 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.

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 could 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 their 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 could 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 [40] 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 and 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.

17. Compliance and Enforcement

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.

Proposed § 164.522(a) would establish the principle that the Secretary would 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.

V. Initial Regulatory Flexibility Analysis

A. Introduction

Pursuant to the Regulatory Flexibility Act 5 U.S.C. 601 *et. seq.*, HHS must prepare a regulatory flexibility analysis if the Secretary certifies that a proposed rule would have a significant economic impact on a substantial number of small entities.

This analysis addresses six issues: (1) Reasons for promulgating the rule; (2) the proposed rule's objectives and legal basis; (3) the number and types of small entities affected by the proposed rule; (4) the specific activities and costs associated with compliance; (5) options that HHS considered to minimize the rule's economic burdens or increase its benefits for small entities; and (6) the relevant Federal rules that could duplicate, overlap, or conflict with the proposed rule. The following sections provide details on each of these issues.

Reasons for Promulgating the Rule

This proposed rule is being promulgated primarily because we have been statutorily mandated to do so under section 264 of Public Law 104–191. Additional information on the reasons for promulgating the rule can be found in earlier preamble discussions (section I.).

Objectives and Legal Basis

This information can be found in earlier preamble discussions (section I.).

Relevant Federal Provisions

This information can be found in earlier preamble discussions (section I.B.)

B. Economic Effects on Small Entities

1. Number and Types of Small Entities Affected

The Small Business Administration defines small entities in the health care sector as those organizations with less than $5 million in annual revenues. [41] Nonprofit organizations are also considered small entities; however, individuals and States are not included in the definition of a small entity. Similarly, small government jurisdictions with a population of less than 50,000 are considered small entities.

Small health entities affected include: Nonprofit health plans, hospitals, and skilled nursing facilities (SNFs); small businesses providing health coverage; small physician practices; pharmacies; laboratories; and durable medical equipment (DME) suppliers; health care clearinghouses; billing companies; and vendors that supply software applications to health care entities.

The U.S. Small Business Administration reports that as of 1996, there were 1,078,020 small health care establishments [42] classified within the SIC codes we have designated (Table A).

[40] 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.

[41] 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 numbers as we used in 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 and also believe that because it is higher than the more recent SBA data, it was the more conservative data source.

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.

[42] Establishments are the physical location where an enterprise conducts business. An entrprise may conduct business in more than one establishment.

TABLE A.—NUMBER OF HEALTH CARE ENTITIES THAT MEET SBA SIZE STANDARDS, 1996 [1]

Standard Industrial Code (SIC)	Industry	Total Number of Health Care Entities	Number of Entities that Meet SBA Size Standards [2]	Percent of Entities that Meet SBA Size Standards [2]
5910	Drug Stores & Proprietary Stores	44,062	23,771	53.9
6320	Accident & Health Insurance & Medical Service Plans (Accident & Health Insurance and Hospital & Medical Service Plans).	3,346	428	12.8
8010	Offices & Clinics of Doctors of Medicine	188,508	171,750	91.1
8020	Offices & Clinics of Dentists	113,965	113,141	99.3
8030	Offices & Clinics of Doctors of Osteopathy	9,168	9,000	98.2
8040	Offices & Clinics of Other Health Practitioners	85,326	83,563	97.9
8050	Nursing & Personal Care Facilities	24,246	11,736	48.4
8060	Hospitals	7,284	837	11.5
8070	Medical & Dental Laboratories	15,354	12,322	80.3
8080	Home Health Care Services	16,218	9,238	57.0
8090	Miscellaneous Health & Allied Services	20,986	12,712	60.6
N/A	Total	528,463	448,498	84.9

[1] Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1996.
[2] Less than $5,000,000 in annual revenue.

These small businesses represent 83.8% of all health care entities we have examined.[43] Small businesses represent a significant portion of the total number of health care entities but a small portion of the revenue stream for all health care entities. In 1996, the small businesses represented generated approximately $235 million in annual receipts, or 22.2% of the total revenue generated by small health care entities (Table B). [44] The following sections provide estimates of the number of small health care entities that will be required to comply with the rule. We should note, however, that the SBA's published annual receipts of health care industries differs substantially from the National health expenditure data that the Health Care Finance Administration (HCFA) maintains. HCFA's data are generally considered more accurate because the data are validated by several sources.

TABLE B.—ANNUAL RECEIPTS OF HEALTH CARE ENTITIES, 1996 [1]

Standard Industrial Code (SIC)	Industry	Total revenue	Revenue generated by small entities [2]	Percent of total revenue generated by small entities
5910	Drug Stores & Proprietary Stores	$91,701,331	$23,762,195	25.9
6320	Accident & Health Insurance & Medical Service Plans (Accident & Health Insurance and Hospital & Medical Service Plans).	225,866,321	657,074	0.3
8010	Offices & Clinics of Doctors of Medicine	186,598,097	102,355,549	54.9
8020	Offices & Clinics of Dentists	46,131,244	44,811,866	97.1
8030	Offices & Clinics of Doctors Of Osteopathy	4,582,835	3,992,558	87.1
8040	Offices & Clinics of Other Health Practitioners	25,053,745	21,891,338	*87.4*
	Other Health Practitioners (8030 and 8040)	29,636,580	25,883,896	87.3
8050	Nursing & Personal Care Facilities	63,625,522	14,672,710	23.1
8060	Hospitals	343,314,509	2,021,845	0.6
8070	Medical & Dental Laboratories	16,543,625	4,976,094	30.1
8080	Home Health Care Services	27,690,537	7,960,035	28.7
8090	Miscellaneous Health & Allied Services	26,036,633	7,697,264	29.6

[43] Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1996.

[44] Op. cit. 1996

[45] Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1996.

[46] Op.cit., 1996

TABLE B.—ANNUAL RECEIPTS OF HEALTH CARE ENTITIES, 1996 [1]—Continued

Standard Industrial Code (SIC)	Industry	Total revenue	Revenue generated by small entities [2]	Percent of total revenue generated by small entities
	Other Health Care Services (8070,8080,8090)	70,270,795	20,633,393	*29.4*
N/A	Total Receipts	1,057,144,399	234,798,528	22.2

[1] Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1996.

[2] The SBA defines a small business as those businesses with less than $5,000,000 in annual revenue. For consistency with the Regulation, we employ the term ''entity'' in place of ''business''.

The Small Business Administration reports that approximately 80 percent of the 15,000 medical laboratories and dental laboratories in the U.S. are small entities.[45] Furthermore, based on HCFA data, we estimate that 98 percent of the 160,000 durable medical equipment suppliers in the U.S. are small entities. Over 90 percent of health practitioner offices are small businesses.[46] Doctor offices (91%), dentist offices (99%), osteopathy (98%) and other health practitioner offices (98%) are primarily considered small businesses.

There are also a small number of hospitals, home health agencies, non-profit nursing facilities, and skilled nursing facilities that will be affected by the proposed rule. According to the American Hospital Association, there are approximately 3,131 nonprofit hospitals nationwide. Additionally, there are 2,788 nonprofit home health agencies in the U.S. The Health Care Finance Administration reports that there are 591 nonprofit nursing facilities and 4,280 nonprofit skilled nursing facilities.[47]

While it is difficult to calculate the number of clearinghouses that meet the definition of a small business, we believe that a significant portion of the 80 health care clearinghouses that process health care claims in the U.S. have annual revenues of less than $5 million annually.[48] We believe that all of the 4,500 billing companies [49] that provide administrative and billing services for physicians' offices have annual revenues below $5 million per year.

Some contractors that work with health care entities will be required to adopt policies and procedures to protect information. We do not expect that the additional burden placed on contractors will be significant. We have not estimated the effect of the proposed rule on these entities because we cannot reasonably anticipate the number or type of contracts affected by the proposed rule. We also do not know the extent to which contractors would be required to modify their policy practices as a result of the rule's implementation.

2. Activities and Costs Associated with Compliance

For a summary of the basic activities that a small entity would need to do to comply with this rule, please refer to section III of the preamble. This discussion summarizes some of the specific activities that covered entities must undertake to comply with the proposed rule's provisions and options considered that would reduce the burden to small entities. In developing this proposed rule, we considered a variety of alternatives for minimizing the economic burden that it will create for small entities. We could not exempt small businesses from the entire proposed rule because they represent such a large and critical proportion of the health care industry (84 percent).

The guiding principle in our considerations of how to address the burden on small entities has been to make provisions scalable. To the extent possible, we have allowed for entities to determine how extensively they will address certain issues. This ability to adapt provisions to minimize burden has been addressed in earlier preamble language and will be briefly discussed again in the following section.

Before discussing specific provisions, it is important to note some of the broader questions that were addressed in formulating this proposed rule. We considered extending the compliance period for small entities but decided that because they represent such a large portion of the health care market, such an extension would be inappropriate. However, HIPAA does create an extended compliance time of 36 months for small plans. For all other time limit questions, we also considered giving small entities the same sort of extensions. For example, entities are required to either approve or deny a request to inspect and copy information within 20 days. We considered allowing small entities a longer response time. Rather than giving small entities extensions, we decided to establish time limits that we believe are reasonable for affected entities of all sizes, with the understanding that larger entities may not need as much time as they have been allocated in certain situations.

While we considered the needs of small entities during our discussions of provisions for this proposed rule, we are highlighting the most significant discussions in the following sections:

a. *Scalability.* Covered entities of all types and sizes would be required to comply with the proposed privacy standards outlined below. The proposed standards would not impose particular mechanisms or procedures that covered entities must adopt to implement the standards. Instead, we would require that each affected entity assess its own needs and devise, implement, and maintain appropriate privacy policies, procedures, and documentation to address its business requirements. How each privacy standard would be satisfied would be business decisions that each entity would have to make. This allows the privacy standards to establish a stable baseline, yet remain flexible enough to take advantage of developments and methods for protecting privacy that will evolve over time.

Because the privacy standards would need to be implemented by all covered entities, from the smallest provider to the largest, multi-state health plan, a single approach to implementing these standards would be neither economically feasible nor effective in safeguarding health information privacy. For example, in a small physician practice the office manager might be designated to serve as the privacy official as one of many duties (see proposed § 164.518(a)) whereas at a large health plan, the privacy official may constitute a full time position and

[45] Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1996.

[46] Op.cit., 1996

[47] Health Care Finance Administration, OSCAR

[48] Faulkner & Gray's *Health Data Directory,* 1999

[49] International Billing Association, 1999

have the regular support and advice of a privacy staff or board.

In taking this approach, we intend to strike a balance between the need to maintain the confidentiality of protected health information and the economic cost of doing so. Health care entities must consider both aspects in devising their solutions. This approach is similar to the approach we proposed in the Notice of Proposed Rulemaking for the administrative simplification security and electronic signature standards.

We decided to use this scaled approach to minimize the burden on all entities with an emphasis on small entities.

b. *Minimum necessary use and disclosure.* The decisions called for in determining what would be the minimum necessary information to accomplish an allowable purpose should include both a respect for the privacy rights of the subjects of the medical record and the reasonable ability of covered entities to delimit the amount of individually identifiable health information in otherwise permitted uses and disclosures. For example, a large enterprise that makes frequent electronic disclosures of similar data would be expected to remove identifiers or to limit the data fields that are disclosed to fit the purpose of the disclosure. An individual physician's office would not be expected to have the same capabilities to limit the amount of information disclosed, although, in the cases of disclosures involving a small number of records, such an office could be expected to hide identifiers or to limit disclosures to certain pages of the medical record that are relevant to the purpose of the disclosure.

We understand that the requirements outlined in this section do not create a bright line test for determining the minimum necessary amount of protected health information appropriate for most uses or disclosures. Because of this lack of precision, we considered eliminating the requirement altogether. We also considered merely requiring covered entities to address the concept within their internal privacy procedures, with no further guidance as to how each covered entity would address the issue. These approaches were rejected because minimizing both the amount of protected health information used and disclosed within the health care system and the number of persons who have access to such information is vital if we are to successfully enhance the confidentiality of people's personal health information. We invite comments on the approach that we have adopted and on alternative methods of implementing the minimum necessary principle.

c. *Right to restrict.* We propose to permit in § 164.506(c) that individuals be able to request that a covered entity restrict further uses and disclosures of protected health information for treatment, payment, or health care operations, and if the covered entity agrees to the requested restrictions, the covered entity may not make uses or disclosures for treatment, payment or health care operations that are inconsistent with such restrictions, unless such uses or disclosures are mandated by law. This provision would not apply to health care provided to an individual on an emergency basis.

It should be noted that there is nothing in this proposed rule that requires a health care provider to agree to a request to restrict uses or disclosures for treatment, payment, or health care operations. Providers who do not wish to, or due to contractual obligations cannot, restrict further use or disclosure are not obligated to treat an individual making a request under this provision.

If small entities view this proposed provision as overly burdensome, they would not have to provide treatment to individuals requesting restrictions. We considered requiring that providers conform to requests to restrict use or disclosures. We rejected this approach due to the potential ethical conflicts these restrictions could pose to health care professionals and the possible burden to providers. Providers comprise a large proportion of the small businesses covered under this proposed regulation.

d. *Creation of de-identified information.* In this rule we are proposing that covered entities and their business partners be permitted to use protected health information to create de-identified health information. Covered entities would be permitted to further use and disclose such de-identified information in any way, provided that they do not disclose the key or other mechanism that would enable the information to be re-identified, and provided that they reasonably believe that such use or disclosure of de-identified information will not result in the use or disclosure of protected health information. This means that a covered entity could not disclose de-identified information to a person if the covered entity reasonably believes that the person would be able to re-identify some or all of that information, unless disclosure of protected health information to such person would be permitted under this proposed rule. In addition, a covered entity could not use or disclose the key to coded identifiers if this rule would not permit the use or disclosure of the identified information to which the key pertains. If a covered entity re-identifies the de-identified information, it may only use or disclose the re-identified information consistent with these proposed rules, as if it were the original protected health information. See proposed § 164.506(d)(1).

As with other components of this proposed rule, removal of identifiers from data could be scaled. Small entities without the resources to determine at what point information is truly de-identified could remove the full list of possible identifiers listed in this regulation. Unless they have reason to believe that the information could still be linked to an individual, this proposed requirement would be fulfilled. However, larger, more sophisticated entities, could choose to determine independently what information needs to be removed.

Furthermore, efforts to remove identifiers from information would be optional. If an entity believes that removing identifiers would be excessively burdensome, it could choose not to release the information or to obtain an authorization from individuals before releasing any information.

e. *Uses and disclosures with individual authorization.* Covered entities must obtain individual authorization to use protected health information for purposes other than those allowed under the proposed rule. Activities requiring authorization would include, for example, marketing and eligibility determinations for health coverage or employment. Costs would be ongoing for staffing and administrative activities related to obtaining authorization from individuals.

In establishing the requirement for covered entities to obtain patient authorization to use individually identifiable health information for purposes other than those allowed under the proposed rule, we decided to include in the proposed rule a model ''request for authorization.'' By following such a model, covered entities, particularly small entities, could avoid the legal and administrative expenses that would be necessary to develop an authorization form that complies with the proposed rule's standards. The proposed rule would not prevent entities from developing their own patient authorization forms or from modifying existing forms in a manner consistent with the model.

The alternative to providing this model would be to state that an authorization would be required and allow entities to develop the authorization. We believe that providing no guidance in this area would have caused unnecessary difficulties and burdens for small entities.

f. *Uses and disclosures permitted without authorization.* This proposed rule would not require any uses or authorizations other than to the subject individual and to the Secretary for compliance. If small entities believe that the costs of making such discretionary disclosures are considered too high, they could choose not to make such disclosures. We would allow all covered entities, but particularly small entities, to base their decisions about these disclosures on any criteria that they believe to be important. We expect that the additional costs related to these disclosures would be factored into their decisions.

In cases where uses or disclosures without authorization are required by other law, we would attempt to minimize costs by not requiring application of the minimum necessary principle.

g. *Notice to individuals of rights and procedures.* The proposed rule would require covered entities to prepare and make available a notice that informs patients about their privacy rights and the entity's actions to protect privacy. Entities that do not already comply with the proposed rule's requirements would incur one-time legal and administrative costs. In addition, plans would incur ongoing costs related to the dissemination of the notice at least once every three years, and all covered entities would have ongoing costs related to dissemination to new individuals requesting services and requests for copies of the notice. Entities would also incur ongoing costs related to answering questions that are associated with the notice.

In discussing the requirement for covered entities to prepare and make available a notice regarding patient privacy rights and the entity's privacy practices, we considered exempting small businesses. Because this would exempt 84 percent of firms, we decided not to create this exemption. The second option would be to exempt extremely small entities. One discussion defined small entities as those with fewer than 10 employees. We decided that informing consumers of their privacy rights and of the activities of covered entities with which they conduct business was too important to exempt any entities.

In addition to requiring a basic notice, we considered requiring a longer more detailed notice that would be available to individuals on request. However, we decided that making information available on request and allowing the covered entity to decide how best to provide such information represents a more balanced approach. We believe that it would be overly burdensome to all entities, especially small entities, to require two notices.

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 receive exactly the same information from each covered plan or provider in the same format and that it would be convenient for covered entities to use a uniform model notice.

There are, however, several disadvantages to this approach. First, and most importantly, no model notice could fully capture the information practices of every covered plan or provider. Large entities will have information practices different from those of small entities. Some health care providers, for example, academic teaching hospitals, might routinely disclose identifiable health information for research purposes. Other health care providers might 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 becomes 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.

We believe that the proposed rule appropriately balances a patient's need for information and assurances regarding privacy with the covered entities' need for flexibility in describing their operations and procedures to protect patient privacy. Instead of a model notice, we have included a sample notice to guide the development of notices. We believe that this is an appropriate way to reduce the burden on all entities including those classified as small.

h. *Administrative requirements for covered entities.* We propose that covered entities be required to implement five basic administrative requirements to safeguard protected health information: designation of a privacy official, the provision of privacy training, establishment of safeguards, a complaint process, and establishment of sanctions. Implementation of these requirements would vary depending on a variety of different factors such as type of entity (*e.g.*, provider or plan), size of entity (*e.g.*, number of employees, number of patients), the level of automation within the entity (*e.g.*, electronic medical records), and organization of the entity (*e.g.*, existence of an office of information systems, affiliation with a medical school).

In proposed § 164.518(a), we would require covered plans and providers to designate a privacy official to be responsible for the development of policies for the use and disclosure of protected health information and for the supervision of personnel with respect to use and disclosure of protected health information. The designation of a privacy official would focus the responsibility for development of privacy policy.

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 an individual whose sole responsibility is privacy policy, and that individual could choose to convene a committee representing several different components of the entity to develop and implement privacy policy.

In proposed § 164.518(b), we would require covered entities to provide training on the their policies and procedures with respect to protected health information. 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.

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.

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. 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.

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. 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.

i. *Documentation requirements for covered entities.* We are proposing that covered entities be required to document policies and procedures in several important areas. These areas would include use within the entity; informing business partners; disclosures with and without authorization; limitations on use and disclosure for self-pay; inspection and copying; amendment or correction; accounting for uses and disclosures; notice development, maintenance, and dissemination; sanctions; and complaint procedures. We considered whether formal documentation of these policies would be necessary. A key factor in making this decision was determining the burden on entities, particularly the burden on small entities. We also considered whether it would be reasonable to exempt very small entities from this provision. For example, entities with fewer than ten employees could be able to effectively communicate policies and procedures verbally. We decided that we needed to include all entities in the provision because these documentation requirements are intended as tools to educate the management, employees, and business partners about the consideration that should be given to protecting the privacy of health information.

3. The Burden on a Typical Small Business.

We expect that small entities will face a cost burden as a result of complying with the proposed regulation. We estimate that the burden of developing privacy policies and procedures is lower in dollar terms for small businesses than for large businesses, but we recognize that the cost of implementing privacy provisions will be a larger burden to small entities as a proportion of total revenue. Due to these concerns, we rely on the principle of scalability stated in the proposed rule, and have based our cost estimates on the expectation that small entities will develop less expensive and less complex privacy measures than large entities.

In many cases, we have specifically considered the impact that the proposed rule may have on solo practitioners or rural providers. Where these providers do not have large technical systems, it is possible that the regulation may not apply to small providers, or that small providers will not be required to change their business practices other than adhering to the basic requirements that they state their privacy policies and notify patients of their privacy rights. For both activities, the proposed regulation accounts for the activities and size of the practice. Scalability implies that in developing policies and procedures to comply with the proposed regulation, businesses should consider their basic functions and the amount of health information exchanged electronically. All covered entities must take appropriate steps to address privacy concerns, and in determining the scope and extent of their compliance activities, businesses should weigh the costs and benefits of alternative approaches and should scale their compliance activities to their structure, functions, and capabilities.

Our analysis of the costs to small businesses is divided into three sections: (1) Initial start-up costs associated with development of privacy policy; (2) initial start-up costs associated with system change; and (3) ongoing costs, including notification of privacy policies.

Overall, our analysis suggests that the average start-up cost of complying with the proposed rule is $396 per entity. This includes the cost of developing privacy policies and systems compliance changes (Table C). The ongoing costs of privacy compliance are approximately $337 per entity in the first year and $343 every year thereafter (Table D). The total cost of implementing initial and ongoing costs of the proposed regulation in the first year is $733 per entity. After the first year, the total compliance cost to the entity is $343 per year. We estimate that the relative average cost of initial compliance is approximately 0.12 percent of a small entity's annual expenditures in the first year. The relative average cost of ongoing privacy compliance is approximately 0.05 percent of a small entity's annual expenditures.

Our cost calculations are based on several assumptions. The cost of developing privacy policies is based on figures from the regulatory impact analysis that accompanied the HIPAA National Provider Identifier (63 FR 25320). The cost of initial systems compliance is based on current assumptions about market behavior; including the assumption that a relatively small proportion of the total cost of system compliance (20%) will be absorbed by small covered entities. We evaluated the ongoing costs of an entity's privacy protection by calculating that privacy protection costs should be proportional to the number of patients served by the business. For example, the cost of notifying patients of privacy practices will be directly proportional to the number of patients served. We then multiplied the proportion of small entities by the total ongoing costs of privacy compliance.

Initial Costs

Table C shows the results of our calculations of the cost of initial compliance. We calculated initial privacy policy costs separate from initial system compliance costs because we made different assumptions about the cost of each. To calculate initial privacy policy costs per small entity, we multiplied the estimated cost of developing privacy policies (per entity) by the number of establishments. We then averaged these costs and computed that the average cost of developing privacy policies is $334.31 per small entity. The average cost of implementing privacy policies is greater than the $300 cost we assume most health care provider offices will pay, because we assume that small health plans, hospitals, and nursing and patient care services will spend between $500–$1,000 to implement privacy policies. Calculating the cost of system compliance per entity required us to estimate the percent of total system costs that each type of entity would incur. We used the $90 million figure (cited in the RIA) as the basis for distributing system compliance costs across various types of entities affected by the proposed rule. We estimated how this cost would be divided between small and large entities, and among plans, providers and clearinghouses.

TABLE C.—ANNUAL COST OF IMPLEMENTING PROVISIONS OF THE PROPOSED PRIVACY REGULATION IN THE FIRST YEAR

Industry	Initial costs				Ongoing costs			Total costs	
	Initial privacy policy costs incurred by small entities, per entity	Initial system compliance cost incurred by small entities [1], per entity	Notice development cost, per small entity	Total initial compliance cost, per small entity [2]	First year notice issuance costs for small entities, per small entity	Annual amendment and correction cost to small entities, per small entity	Annual written authorization cost to small entities, per small entity	Total annual ongoing cost in the first year, per small entity	Total annual initial and ongoing cost in the first year, per small entity
Drug Stores & Proprietary Stores [3]	$300	$131.19	$59.40	$490.58	$118.26	$768.64	$102.55	$989.45	$1,480.03
Accident & Health Insurance & Medical Service Plans [3] (Accident & Health Insurance and Hospital & Medical Service Plans)	1,000	1,939.86	203.91	3,143.77	314.02	127.60	17.02	458.65	3,602.41
Offices & Clinics Of Doctors Of Medicine	300	21.04	21.20	342.24	42.21	260.93	34.81	337.96	680.20
Offices & Clinics Of Dentists	300	7.43	13.25	320.68	26.39	163.11	21.76	211.26	531.94
Offices & Clinics Of Other Health Practitioners	300	11.10	17.82	328.92	35.47	219.29	29.26	284.02	612.94
Nursing & Personal Care Facilities	1,500	117.15	49.63	1,666.79	98.82	610.88	81.50	791.20	2,457.99
Hospitals	1,500	7,362.22	79.65	8,941.87	158.59	980.36	130.80	1,269.75	10,211.62
Home Health Care Services	300	58.06	30.66	388.72	61.05	377.38	50.35	488.77	877.49
Other Health Care Services including Lab Services	300	19.83	10.84	330.68	21.59	133.47	17.81	172.87	503.55
Average Cost	334.31	40.13	21.17	395.61	42.05	260.23	34.72	337.00	732.61

[1] The SBA defines small health care entities as those with annual revenue under $5,000,000.
[2] Total Initial Compliance Cost includes policy implementation and systems compliance costs.
[3] Includes some entities not covered by this regulation. Pharmacies are the only component of Drug Stores and Proprietary Stores covered by the regulation. Accident and workers compensation insurance are not covered by the regulation.

TABLE D.—ANNUAL COST OF IMPLEMENTING PROVISIONS OF THE PROPOSED PRIVACY REGULATION, AFTER THE FIRST YEAR

Industry	Ongoing Costs				
	Annual notice issuance costs after the first year, per small entity	Annual amendment and correction cost to small entities, per small entity	Annual written authorization cost to small entities, per small entity	Annual ongoing costs for paperwork and training, per small entity	Total annual ongoing cost after the first year, per small entity
Drug Stores & Proprietary Stores [1]	73.26	768.64	102.55	20	964.45
Accident & Health Insurance & Medical Service Plans [2] (Accident & Health Insurance and Hospital & Medical Service Plans)	314.02	127.60	17.02	60	518.65
Offices & Clinics Of Doctors Of Medicine	26.15	260.93	34.81	20	341.90
Offices & Clinics Of Dentists	16.35	163.11	21.76	20	221.22
Offices & Clinics Of Other Health Practitioners	21.97	219.29	29.26	20	290.52
Nursing & Personal Care Facilities	61.22	610.88	81.50	100	853.59
Hospitals	98.24	980.36	130.80	100	1,309.40
Home Health Care Services	37.82	377.38	50.35	20	485.54
Other Health Care Services including Lab Services	13.38	133.47	17.81	20	184.65
Average Cost	26.16	260.23	34.72	22.28	343.39

[1] The SBA defines small health care entities as those with annual revenue under $5,000,000.
[2] Includes some entities not covered by this regulation. Pharmacies are the only component of Drug Stores and Proprietary Stores covered by the regulation. Accident and workers compensation insurance are not covered by the regulation.

Our calculations regarding division of costs are based on two assumptions: (1) System costs are principally fixed costs associated with the purchase of hardware and software [50]; and (2) large entities will continue to invest more heavily in hardware and software expenditures than small entities. We estimate that 80 percent of the system costs will be born by large entities. The remaining 20 percent of total systems costs will be absorbed by small entities. To calculate the effect on small businesses, we multiplied the system compliance costs cited in the RIA by the proportion of the costs we expect small entities to incur (20 percent of total). We then multiplied the total cost of system compliance for small entities by the percentage of health care revenue by industry and calculated a cost per entity.

We used HCFA's estimate of total national health expenditures to calculate the percent of total health care business that is represented by types of health care entities. We calculated the proportion of business transacted by a type of health care entity (by SIC code) and multiplied this by the total expenditures ($1.084 billion total) [51]. National expenditure data is a useful measure for allocating system compliance costs for two reasons. Even though system compliance costs are primarily fixed costs, we assume that they bear some relationship to the size and level of the activity of the entity.

[50] We are not suggesting that these investments are exclusively computer-related. They may also include costs for personnel training, reorganization, and contract negotiations with outside entities.

[51] Health Care Finance Administration, 1996 http://www.hcfa.gov/stats/nheoact/tables/t10.htm

Similarly, national expenditures vary according to both size and level of activity. Second, in contrast to the annual receipts compiled by the Business Census Survey, national expenditure information compares its data to other sources in order to validate its results. Thus, we decided that the national expenditure data are a more reliable source of overall business activity for our purposes. Based on these assumptions, we believe that the total cost of system compliance for all small health care entities will be approximately 18 million. Dividing costs by the number of small entities suggests that the average cost of system compliance is $40.13 per entity.

The cost of notice development is approximately $21 per small entity. We assume that many small providers will receive assistance developing their notice policies from professional associations. Thus, the overall cost of developing compliant notices is significant, but the cost per entity is small. The cost to small entities of developing notices is based on the proportion of expenditures generated by small entities. We recognize that this may not adequately capture the costs of developing a provider or plan's notice of their privacy policies, and invite comment on our approach.

We added the per-entity cost of privacy policy implementation to the cost of systems compliance to determine the total average cost of start-up compliance. Our figures indicate that initial compliance will cost an average of $396 per small entity. These costs vary across entity type (Table C). For example, small hospitals have a much higher cost of compliance than the average cost for all small entities, whereas dentists' offices tend to have initial compliance costs that are lower than the average for small entities. Most small practitioner offices have low costs ($320 per dentist office), whereas small hospitals ($8,942 per entity) and small insurance companies have much higher costs ($3,144 per entity) than other health care entities.

Finally, we attempted to estimate the impact of compliance costs on small entities by comparing the cost of complying with the proposed rule to an entity's annual expenditures (Table E). We computed the percent of small entity expenditures as a percent of national expenditures by calculating the proportion of small business receipts (from census data compiled for the SBA) that apply to segments of the health care market. Although we believe that the SBA data understates the amount of annual receipts, we assumed that the underestimates are consistent across all entities. Thus, although the dollar amounts reported by the SBA are incorrect, our assumption is that the proportion of small entity receipts relative to total annual receipts is correct.

Applying the percent of small entity receipts to the national expenditure data allows us to estimate the percent of national expenditures represented by small entities. We then considered the total compliance cost (initial and ongoing cost) as a percent of small business expenditures. Our estimates suggest that the cost of complying with the proposed rule represent approximately 0.12 percent of total annual expenditures for a small health care entity in the first year. The relative cost of complying with the proposed rule is substantially lower in subsequent years, representing 0.04 percent of an entity's annual expenditures. The relative cost of complying with the proposed regulation cost of complying is highest for small health insurers (1.03 percent of expenditures). These costs will be higher due to the volume and complexity of health plan billing systems; health plans are required to implement more policies and procedures to protect health information because they handle so much personally identifiable information. Because health plan costs are higher and there is a smaller number of plans than other type of entities affected by the regulation, these costs result in a higher annual cost per small health plan. Table E further illustrates the cost impact by type of entity in the first year.

TABLE E.—SMALL ENTITY BUSINESS EXPENDITURES AND PROPORTION OF ANNUAL EXPENDITURES REPRESENTED BY INITIAL AND ONGOING COMPLIANCE COSTS IN THE FIRST YEAR *

Industry	Total annual initial and ongoing costs in the first year, per small entity	Annual expenditure per small entity [1]	Compliance cost as a percentage of a small entity's annual expenditures
Drug Stores & Proprietary Stores [2]	$1,480.03	$2,046,199	0.07
Accident & Health Insurance & Medical Service Plans [2] (Accident & Health Insurance and Hospital & Medical Service Plans)	3,602.41	350,467	1.03
Offices & Clinics Of Doctors Of Medicine	680.20	695,560	0.10
Offices & Clinics Of Dentists	531.94	434,260	0.12
Offices & Clinics Of Other Health Practitioners	612.94	583,805	0.10
Nursing & Personal Care Facilities	2,457.99	1,629,755	0.15
Hospitals	10,211.62	2,660,215	0.38
Home Health Care Services	877.49	1,003,475	0.09
Other Health Care Services including Lab Services	503.55	351,146	0.14
Average Cost	732.61	625,992	0.12

* The SBA defines small health care entities as those with annual revenue under $5,000,000.
** Total Initial Compliance Cost includes policy implementation and systems compliance costs
[1] Based on the assumption that the proportion of revenue generated by small businesses approximates the proportion of expenditures faced by small businesses
[2] Includes some entities not covered by this regulation. Pharmacies are the only component of Drug Stores and Proprietary Stores covered by the regulation. Accident and workers compensation insurance are not covered by the regulation.

Ongoing Costs

In this section, we evaluate the ongoing costs of providing patient notices, the annual cost of amending and correcting medical information, the cost of providing written authorizations, and the ongoing cost of paperwork and training. We estimated the ongoing costs of compliance through calculations similar to those used for our systems compliance estimates. Ongoing costs are most heavily influenced by the size of the business. Therefore, we assume that the number of patients an entity serves is directly proportional to its ongoing compliance costs.

We estimated market share using Small Business Administration data estimating total receipts.[52] We divided the small entity receipts by total receipts and arrived at an estimate that 22 percent of the revenue generated by the health care classifications we examined is from small businesses. Using annual receipts to estimate cost burden is more accurate than using information on the number of health care entities. The size of the small entity is more likely to be correlated with the number of patients served than the number of businesses, and therefore, the amount of business conducted by an entity. Because it is difficult to find a single good estimate of market share, we considered estimating market share over a range, using the proportion of annual receipts as a lower bound and number of entities as the higher bound. We concluded that even if the SBA data does not capture the total amount of health care receipts accurately, estimating market share by examining receipts would be much more accurate than using the number of entities.

We multiplied the percent total receipts by the total ongoing costs (by entity type) to obtain a range of ongoing costs for small entities. We were then able to divide these costs by the number of small entities by type of entity. We estimated ongoing costs in the first year that the proposed rule takes effect separately from our estimate of ongoing cost in the following years. The estimates were approximately the same; $337 and $343 respectively.

We estimate that the ongoing cost of compliance will be approximately 0.05 percent of a small entity's annual expenditures. This cost burden is fairly consistent across all types of entities.

Clearinghouses and Nonprofit Entities

We should note that the above discussion does not consider health care clearinghouses, nonprofit hospitals, home health agencies, or nursing and skilled nursing facilities. To the extent that clearinghouses and nonprofit facilities have annual receipts of less than $5 million, they were included in the preceding analysis.

Although we do not have precise information on the number of clearinghouses that qualify as small entities under the RFA, we believe that approximately half would meet the criteria. As noted in the regulatory impact analysis, as long as clearinghouses perform the function of merely reformatting information they receive and transmitting the data to other entities, the cost of complying with the proposed rule should be minimal.

A similar logic applies for nonprofit health plans and hospitals. We do know how many nonprofit organizations currently exist in the U.S., but do not have reliable revenue and expenditure data for these entities. In the absence of such data, we assume that nonprofit entities have a similar ratio of revenues to expenditures as the for-profit entities we have examined. Thus, we believe that the impact of complying with the proposed rule should be similar to that described for-profit plans and hospitals.

The preceding analysis indicates that the expected burden on small entities of implementing the proposed rule would be minimal. However, by necessity, the analysis is based on average costs, and as such, they may not reflect the actual burden on some or even a substantial number of small entities. Therefore, the Secretary does not certify that the proposed rule will not have a significant impact on a substantial number of small entities.

VI. Unfunded Mandates

The Unfunded Mandates Reform Act of 1995 (Pub. L. 104–4) requires cost-benefit and other analyses for rules that would cost more than $100 million in a single year. The proposed rule qualifies as a significant rule under the statute. DHHS has carried out the cost-benefit analysis in sections D and E of this document, which includes a discussion of unfunded costs to the states resulting from this regulation.

A. Future Costs

DHHS estimates some of the future costs of the proposed rule in Section E of the Preliminary Regulatory Impact Analysis of this document. The reported costs include costs incurred during the compliance period and up to 5 years after the effective date. The same section also includes some qualitative discussion of costs that would occur beyond that time period. Most of the costs of the proposed rule, however, would occur in the years immediately after the publication of a final rule. Future costs beyond the five year period will continue but will not be as great as the initial compliance costs.

B. Particular Regions, Communities, or Industrial Sectors.

The proposed rule applies to the health care industry and would, therefore, affect that industry disproportionately. Any long-run increase in the costs of health care services would largely be passed on to the entire population of consumers.

C. National Productivity and Economic Growth

The proposed rule is not expected to substantially affect productivity or economic growth. It is possible that productivity and growth in certain sectors of the health care industry could be slightly lower than otherwise because of the need to divert research and development resources to compliance activities. The diversion of resources to compliance activities would be temporary. Moreover, DHHS anticipates that, because the benefits of privacy are large, both productivity and economic growth would be higher than in the absence of the proposed rule. In section I.A. of this document, DHHS discusses its expectation that this proposed rule would increase communication among consumers, health plans, and providers and that implementation of privacy protections will lead more people to seek health care. The increased health of the population will lead to increased productivity and economic growth.

D. Full Employment and Job Creation.

Some of the human resources devoted to delivery of health care services would be redirected by the proposed rule. The proposed rule could lead to some short-run changes in employment patterns as a result of the structural changes within the health care industry. The growth of employment (job creation) for the roles typically associated with the health care profession could also be temporarily change but be balanced by an increased need for those who can assist entities with complying with this proposed rule. Therefore, while there could be a temporary slowing of growth in traditional health care professions, that will be offset by a temporary increase in growth in fields that may assist with compliance with this proposed rule (e.g. legal professionals, and management consultants).

E. Exports

Because the proposed rule does not mandate any changes in products, current export products will not be required to change in any way.

VII. Environmental Impact

The Department has determined under 21 CFR 25.30(K) that this action

[52] Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1996.

is of a type that does not individually or cumulatively have a significant effect on the human environment. Therefore, neither an environmental assessment nor an environmental impact statement is required.

VIII. Collection of Information Requirements

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

• Whether the information collection is necessary and useful to carry out the proper functions of the agency;
• The accuracy of the agency's estimate of the information collection burden;
• The quality, utility, and clarity of the information to be collected; and
• Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

Under the PRA, the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section are to be considered. Due to the complexity of this regulation, and to avoid redundancy of effort, we are referring readers to Section IV (Regulatory Impact Analysis) above, to review the *detailed* cost assumptions associated with these PRA requirements. We explicitly seek, and will consider public comment on our cost assumptions, as they relate to the PRA requirements summarized in this section.

SUMMARY PRA BURDEN HOURS

Provision	Burden (in hours)
§ 160.204 Process for requesting exceptions.	160
§ 164.506 General standards and implementation specifications for uses and disclosures of protected health information.	* TBD
§ 164.508 Standards and implementation specifications for uses and disclosures for which individual authorization would be required.	3,561,076
§ 164.510 Standards and implementation specifications for uses and disclosures for which individual authorization would not be required.	8,903
§ 164.512 Notice of privacy practices; rights and procedures.	7,273,952
§ 164.514 Access to protected health information; rights and procedures.	* TBD
§ 164.515 Accounting for uses and disclosures of protected health information	* TBD
§ 164.516 Amendment and correction; rights and procedures	*TBD
§ 164.520 Development and documentation of policies and procedures	2,927,000
§ 164.522 Compliance and Enforcement	2,500
Total Hours	13,773,591

* Burden to be determined based upon public comment.

Section 160.204 Process for Requesting Exceptions.

Section 160.204 would require States to: (1) Submit a written request, that meets the requirements of this section, to the Secretary to except a provision of State law from preemption under § 160.203; (2) submit a new request to the Secretary, should there be any changes to the standard, requirement, or implementation specification or provision of State law upon which an exception previously was granted, and (3) submit a written request for an extension of the exception prior to the end of the three-year approval period for a given exception. In addition, § 160.204 would require a State to submit a written request for an advisory opinion to the Secretary that meets the requirements of § 160.204.

The burden associated with these requirements is the time and effort necessary for a State to prepare and submit the written request for preemption or advisory opinion to HCFA for approval. On an annual basis it is estimated that it will take 10 States 16 hours each to prepare and submit a request. The total annual burden associated with this requirement is 160 hours.

Section 164.506 General Standards and Implementation Specifications for Uses and Disclosures of Protected Health Information

Given that the burden associated with the following information collection requirements will differ significantly, by the type and size of plan or provider, we are explicitly soliciting comment on the burden associated with the following requirements:

• Except for disclosures of protected health information by a covered entity that is a health care provider to another health care provider for treatment purposes, § 160.204(e) would require a covered entity to maintain documentation demonstrating that they have entered into a contract that meets the requirements of this part with each of their business partners;

• A covered entity would have to make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose of the use or disclosure;

• A covered entity could use protected health information to create de-identified information if the individually identifiable information has been removed, coded, encrypted, or otherwise eliminated or concealed.

Section 164.508 Standards and Implementation Specifications for Uses and Disclosures for Which Individual Authorization Would Be Required

Pursuant to the conditions set forth in this section, a covered entity would need to obtain a written request from an individual, before it uses or discloses protected health information of an individual. A copy of the model form which appears in Appendix to Subpart E of Part 164, or a form that contains the elements listed in paragraphs (c) or (d) of this section, as applicable, would need to be accepted by the covered entity.

The burden associated with these proposed requirements is the time and effort necessary for a covered entity to obtain written authorization prior to the disclosure of identifiable information. On an annual basis it is estimated that it will take 890,269 entities, a range of 0 to 80 hours per entity to obtain and maintain authorization documentation on an annual basis. Given that we believe the majority of the covered entities will be minimally affected by this requirement, we estimate the annual average burden per entity to be 4 hours for a total annual burden of 3,561,076 hours. Collecting such authorization should have costs on the order of those associated with providing access to records (not on a per page basis). Since the proposed requirement does not apply to treatment and payment, assuming 1% of the 543 million health care encounters might be reasonable. At a cost of about $10 each, the aggregate cost would be about $54 million. Therefore, on average the cost per entity would be about $60, with many entities receiving no requests and thus having no costs.

Section 164.510 Standards and Implementation Specifications for Uses and Disclosures for Which Individual Authorization Would Not Be Required

A covered entity could disclose protected health information to a health researcher for health research purposes subject to 45 CFR part 46 and purposes other than those subject to 45 CFR part 46, provided that the covered entity has obtained written documentation demonstrating that the applicable requirements proposed in this section have been met.

The burden associated with these proposed requirements is the time and effort necessary for a covered entity to maintain documentation demonstrating that they have obtained institutional review board or privacy board approval, which meet the requirements of this section. On an annual basis it is estimated that this proposed requirement will affect 1 % or 8,903 of covered entities. We further estimate that it will take an average of 1 hour per entity to meet these proposed requirements on an annual basis. Therefore, the total estimated annual burden associated with this proposed requirement is 8,903 hours.

Section 164.512 Notice of Privacy Practices; Rights and Procedures

Section 164.512 would require covered entities to provide written notice of the entities' privacy practices, rights, and procedures that meet the requirements of this section to affected parties upon request and as summarized below.

Health plans would provide a copy of the notice to an individual covered by the plan at enrollment and whenever the content of the notice is significantly altered thereafter, but no less frequently than once every three years. Total notice counts are estimated to be about 230 million, assuming plans choose to send them out annually rather than keeping track of duration since last notice. The average number of notices per plan per year would be about 1,200. For the approximately 19,000 plans issuing notices, the number of notices can be as few as 1,000 for a small self-insured self-administered employer, or as many as a million or more for a large commercial insurer or HMO. We further estimate that it will require each plan, on average, 8 hours to disseminate the required notices. This estimate is based upon the assumption that the required notice will be incorporated and disseminated with a plan's annual policy materials. The total burden associated with this requirement is calculated to be 151,800 hours.

Health care providers would provide a copy of the notice to an individual at the time of first service delivery to the individual, provide as promptly as possible a copy of the notice to an individual served by the provider whenever the content of the notice is significantly altered, post a copy of the notice in a location where it is reasonable to expect individuals seeking services from the provider to be able to read the notice, and date each version of the notice. Total notices in the first year are estimated to be about 700 million (based on annual patient contacts with hospitals, physicians, and other providers), with subsequent year counts of 350 million. Small providers could be providing 400 or fewer notices (based on 150 million persons with ambulatory physician contacts per year and approximately 370,000 physician offices). The overall average will also be close to that amount, since the bulk of providers are small entities. Large providers could be sending out 3,000 or more notices (based on 20 million persons with hospitalizations and approximately 6600 hospitals). We further estimate that it will require each provider, on average, 8 hours to disseminate the required notices. This estimate is based upon the assumption that the required notice will be incorporated into and disseminated with other patient materials. The total burden associated with this requirement is calculated to be 7,122,152 hours.

Section 164.514 Access of Individuals to Protected Health Information

Given that the burden associated with the following information collection requirements will differ significantly, by the type and size of plan or provider, we are explicitly soliciting comment on the burden associated with the following proposed requirements:

- An individual has a right of access to, which includes a right to inspect and obtain a copy of, his or her protected health information in a designated record set of a covered entity that is a health plan or a health care provider, including such information in a business partner's designated record set that is not a duplicate of the information held by the provider or plan, for so long as the information is maintained;
- Where the request is denied in whole or in part, the health plan or a health care provider would provide the individual with a written statement of the basis for the denial and a description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.518 or to the Secretary pursuant to the procedures established in § 164.522 of this subpart.

Section 164.515 Accounting for Uses and Disclosures of Protected Health Information

Given that the burden associated with maintaining records to facilitate the recreation of disclosures will differ significantly, be the type and size of plan or provider, we are explicitly soliciting comment on the burden associated with the following proposed record keeping requirement:

- A covered entity that is a plan or provider would need to be able to give individuals an accurate accounting of all uses and disclosures that are for purposes other than treatment, payment, and health care operations; except that such procedures would provide for the exclusion from such accounting of protected health information which is disclosed to a health oversight or law enforcement agency, if the health oversight or law enforcement agency provides a written request stating that the exclusion is necessary because disclosure would be reasonably likely to impede the agency's activities and specifies the time for which such exclusion is required.

Section 164.516 Amendment and Correction

Given that burden will associated with the following information collection requirements will differ significantly, by the type and size of plan or provider, we are explicitly soliciting comment on the burden associated with the following proposed requirements:

- An individual would have the right to request amendment or correction of his or her protected health information in designated records created by a covered entity that is a health plan or health care provider, where the individual asserts that the information is not accurate or complete and where the error or omission may have an adverse effect on the individual.

• Where the request is denied , provide the individual with a written statement of the basis for the denial, a description of how the individual may file a statement of disagreement with the denial, a description of how the individual may file a complaint with the covered entity, including the name and telephone number of a contact person within the covered entity who can answer questions concerning the denial and the complaint process; and a description of how the individual may file a complaint with the Secretary pursuant to § 164.522 of this subpart.

Section 164.520 Internal Privacy Practices; Standards and Procedures

A covered entity would need to ensure that all employees who have access to protected health information have received appropriate training about the entity's policies for use and disclosure of such information. Upon completion of the training and at least once every three years thereafter, covered entities would require each employee to sign a statement that he or she received the privacy training and will honor all of the entity's privacy policies and procedures.

The burden associated with these requirements is the time and effort necessary for a covered entity to obtain and maintain certification documentation demonstrating that applicable employees have received privacy training and will honor all of the entity's privacy policies and procedures. It is estimated that it will take 890,269 entities, a range of 1 hour to 40 hours per entity to obtain and maintain documentation on an annual basis. Given that we believe the majority of the covered entities will be minimally affected by this requirement, we estimate the annual average burden to be 3 hours per entity for a total annual burden of 2,700,000 hours. Using previous calculations, 900,000 (rounded) entities break down to about 95% small, 5% various types of large, and 1 burden hour for 95%, and 40 burden hours for 5%, the average burden would be 3 hours.

In addition, this section would require a covered entity that is a health plan or health care provider to develop and document its policies and procedures for implementing the requirements of this proposed rule, and amend the documentation to reflect any change to a policy or procedure.

The burden associated with these requirements is the time and effort necessary for a covered entity to maintain documentation demonstrating that they have implemented procedures that meet the requirements of this proposed rule. It is estimated that it will take 890,269 entities a range of 15 minutes to 1 hour per entity to maintain procedural documentation on an annual basis. We believe the majority (95%) of the covered entities will be minimally affected by this requirement. Using the 95% small/5% large, the average burden is 17 minutes. Multiplying by 890,269, results in a total annual burden of 256,000 hours (see discussion below).

Since the requirements for developing formal processes and documentation of procedures mirror what will already have been required under the HIPAA security regulations, the burden and additional costs should be small. To the extent that national or state associations will develop guidelines or general sets of processes and procedures which will be reviewed by individual member entity, the costs would be primarily those of the individual reviewers. Assuming this process occurs, we believe that entities will review information from associations in each state and prepare a set of written policies to meet their needs. Our estimates are based on assumed costs for providers ranging from $300 to $3000, with the average being about $375. The range correlates to the size and complexity of the provider. With less than 1 million provider entities, the aggregate cost would be on the order of $300 million. For plans and clearinghouses, 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. We believe the costs for these entities will range from $300 for smaller plans to $15,000 for the largest plans. Because there are very few large plans in relation to the number of small plans, the average implementation costs will be about $3050.

Section 164.522 Compliance and Enforcement

An individual who believes that a covered entity is not complying with the requirements of this subpart may file a complaint with the Secretary within 180 days from the date of the alleged non-compliance, unless the time for filing is extended by the Secretary. The complaint would describe in detail the acts or omissions believed to be in violation of the requirements of this subpart.

The burden associated with these requirements is the time and effort necessary for an individual to prepare and submit a written complaint to the Secretary. On an annual basis it is estimated that 10,000 complaints will be filed on an annual basis. We further estimate that it will take an average of 15 minutes per individual to submit a complaint. Therefore, the total estimated annual burden associated with this requirement is 2,500 hours.

A covered entity would need to maintain documentation necessary for the Secretary to ascertain whether the covered entity has complied or is complying with the requirements of this subpart. While this section is subject to the PRA, the burden associated with this requirement is addressed under sections referenced above, which discuss specific record keeping requirements.

We have submitted a copy of this proposed rule to OMB for its review of the information collection requirements in §§ 160.204, 164.506, 164.508, 164.510, 164.512, 164.514, 164.515, 164.516, 164.520, and § 164.522. These requirements are not effective until they have been approved by OMB.

If you comment on any of these information collection and record keeping requirements, please mail copies directly to the following:

Health Care Financing Administration, Office of Information Services, Information Technology Investment Management Group, Division of HCFA Enterprise Standards, Room C2–26–17, 7500 Security Boulevard, Baltimore, MD 21244–1850. ATTN: John Burke HIPAA Privacy-P

Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10235, New Executive Office Building, Washington, DC 20503. ATTN: Allison Herron Eydt, HCFA Desk Officer.

IX. Executive Order 12612: Federalism

The Department has examined the effects of provisions in the proposed privacy regulation on the relationship between the Federal government and the States, as required by Executive Order 12612 on ''Federalism.'' The agency concludes that preempting State or local proposed rules that provide less stringent privacy protection requirements than Federal law is consistent with this Executive Order. Overall, the proposed rule attempts to balance both the autonomy of the States with the necessity to create a Federal benchmark to preserve the privacy of personally identifiable health information.

It is recognized that the States generally have laws that relate to the privacy of individually identifiable health information. The HIPAA statute dictates the relationship between State law and this proposed rule. Except for laws that are specifically exempted by the HIPAA statute, State laws continue to be enforceable, unless they are contrary to Part C of Title XI of the standards, requirements, or implementation specifications adopted or pursuant to subpart x. However, 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.

Section 3(b) of Executive Order 12612 recognizes that Federal action limiting the discretion of State and local governments is appropriate ''where constitutional authority for the action is clear and certain and the national activity is necessitated by the presence of a problem of national scope.'' Personal privacy issues are widely identified as a national concern by virtue of the scope of interstate health commerce. HIPAA's provisions reflect this position. HIPAA attempts to facilitate the electronic exchange of financial and administrative health plan transactions while recognizing challenges that local, national, and international information sharing raise to confidentiality and privacy of health information.

Section 3(d)(2) of the Executive Order 12612 requires that the Federal government refrain from ''establishing uniform, national standards for programs and, when possible, defer to the States to establish standards.'' HIPAA requires HHS to establish standards, and we have done so accordingly. This approach is a key component of the proposed privacy rule, and it adheres to Section 4(a) of Executive Order 12612, which expressly contemplates preemption when there is a conflict between exercising State and Federal authority under Federal statute. Section 262 of HIPAA enacted Section 1178 of the Social Security Act, developing a ''general rule'' that State laws or 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. Several exceptions to this rule exist, each of which is designed to maintain a high degree of State autonomy.

Moreover, Section 4(b) of the Executive Order authorizes preemption of State law in the Federal rule making context when there is ''firm and palpable evidence compelling the conclusion that the Congress intended to delegate to the * * * agency the authority to issue regulations preempting State law.'' Section 1178 (a)(2)(B) of HIPAA specifically preempts State laws related to the privacy of individually identifiable health information unless the State law is more stringent. Thus, we have interpreted State and local laws and regulations that would impose less stringent requirements for protection of individually identifiable health information as undermining the agency's goal of ensuring that all patients who receive medical services are assured a minimum level of personal privacy. Particularly where the absence of privacy protection undermines an individual's access to health care services, both the personal and public interest is served by establishing Federal rules.

The proposed rule would establish national minimum standards with respect to the collection, maintenance, access, transfer, and disclosure of personally identifiable health information. The Federal law will preempt State law only where State and Federal laws are ''contradictory'' and the Federal regulation is judged to establish ''more stringent'' privacy protections than State laws.

As required by the Executive Order, States and local governments will be given, through this notice of proposed rule making, an opportunity to participate in the proceedings to preempt State and local laws (section 4(e) of Executive Order 12612). However, it should be noted that the preemption of state law is based on the HIPAA statute. The Secretary will also provide a review of preemption issues upon requests from States. In addition, under the Order, appropriate officials and organizations will be consulted before this proposed action is implemented (section 3(a) of Executive Order 12612).

Finally, we have considered the cost burden that this proposed rule would impose on State-operated health care entities, Medicaid, and other State health benefits programs. We do not have access to reliable information on the number of State-operated entities and programs, nor do we have access to data on the costs these entities and programs would incur in order to comply with the proposed rule. A discussion of possible compliance costs that covered entities may incur is contained in the Unfunded Mandates section above. We believe that requiring State health care entities covered by the proposed rule to comply with the proposed rule would cost less than one percent of a State's annual budget.

The agency concludes that the policy proposed in this document has been assessed in light of the principles, criteria, and requirements in Executive Order 12612; that this policy is not inconsistent with that Order; that this policy will not impose significant additional costs and burdens on the States; and that this policy will not affect the ability of the States to discharge traditional State governmental functions.

During our consultation with the States, representatives from various State agencies and offices expressed concern that the proposed regulation would pre-empt all State privacy laws. As explained in this section, the regulation would only pre-empt state laws where there is a direct conflict between state laws and the regulation, and where the regulation provides more stringent privacy protection than State law. We discussed this issue during our consultation with State representatives, who generally accepted our approach to the preemption issue. During the consultation, we requested further information from the States about whether they currently have laws requiring that providers have a ''duty to warn'' family members or third parties about a patient's condition other than in emergency circumstances. Since the consultation, we have not received additional comments or questions from the States.

X. Executive Order 13086: Consultation and Coordination with Indian Tribal Governments

In drafting the proposed rule, the Department consulted with representatives of the National Congress of American Indians and the National Indian Health Board, as well as with a representative of the self-governance Tribes. During the consultation, we discussed issues regarding the application of Title II of HIPAA to the Tribes, and potential variations based on the relationship of each Tribe with the IHS for the purpose of providing health services. Participants raised questions about the status of Tribal laws regarding the privacy of health information.

List of Subjects in 45 CFR Parts 160 and 164

Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Medicaid, Medical research, Medicare, Privacy, Reporting and recordkeeping requirements, security measures.

Note to reader: This proposed rule is one of several proposed rules that are being published to implement the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996. We propose to establish a new 45 CFR subchapter C, parts 160 through 164. Part 160 will consist of general provisions, part 162 will consists of the various Administrative Simplification regulations relating to transactions and identifiers, and part 164 will consists of the regulations implementing the security and privacy requirements of the legislation. Proposed part 160, consisting of two subparts (Subpart A General Provisions, and Subpart B—Preemption of State Law) will be exactly the same in each rule, unless we add new sections or definitions to incorporate additional general information in the later rules.

Dated: October 26, 1999.

Donna Shalala,

Secretary.

Appendix to the Preamble: Sample Contact of Provider Notice

PROVIDER NOTICE OF INFORMATION PRACTICES (as of 1/1/1999)

Uses and Disclosures of Health Information

We use health information about you for treatment, to obtain payment for treatment, for administrative purposes, and to evaluate the quality of care that you receive.

We may use or disclose identifiable health information about you without your authorization for several other reasons. Subject to certain requirements, we may give out health information without your authorization for public health purposes, for auditing purposes, for research studies, and for emergencies. We provide information when otherwise required by law, such as for law enforcement in specific circumstances. In any other situation, we will ask for your written authorization before using or disclosing any identifiable health information about you. If you choose to sign an authorization to disclose information, you can later revoke that authorization to stop any future uses and disclosures.

We may change our policies at any time. Before we make a significant change in our policies, we will change our notice and post the new notice in the waiting area and in each examination room. You can also request a copy of our notice at any time. For more information about our privacy practices, contact the person listed below.

Individual Rights

In most cases, you have the right to look at or get a copy of health information about you that we use to make decisions about you. If you request copies, we will charge you $0.05 (5 cents) for each page. You also have the right to receive a list of instances where we have disclosed health information about you for reasons other than treatment, payment or related administrative purposes. If you believe that information in your record is incorrect or if important information is missing, you have the right to request that we correct the existing information or add the missing information.

You may request in writing that we not use or disclose your information for treatment, payment and administrative purposes except when specifically authorized by you, when required by law, or in emergency circumstances. We will consider your request but are not legally required to accept it.

Complaints

If you are concerned that we have violated your privacy rights, or you disagree with a decision we made about access to your records, you may contact the person listed below. You also may send a written complaint to the U.S. Department of Health and Human Services. The person listed below can provide you with the appropriate address upon request.

Our Legal Duty

We are required by law to protect the privacy of your information, provide this notice about our information practices, and follow the information practices that are described in this notice.

If you have any questions or complaints, please contact: Office Administrator, 111 Main Street, Suite 101, Anytown, OH 41111. Phone: (111) 555–6789, Email: admin@docshop.com.

For the reasons set forth in the preamble, it is proposed to amend 45 CFR subtitle A by adding a new subchapter C, consisting of parts 160 through 164, to read as follows:

SUBCHAPTER C—ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS

Part

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

Subpart A—General Provisions

Sec.

Subpart B—Preemption of State Law

Authority: 42 U.S.C. 1320d–2 and 1320d–4.

Subpart A—General Provisions

§ 160.101 Statutory basis and purpose.

The requirements of this subchapter implement sections 1171 through 1179 of the Social Security Act, as amended, which require HHS to adopt national standards to enable the electronic exchange of health information in the health care system. The requirements of this subchapter also implement section 264 of Pub. L 104–191, which requires that HHS adopt national standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a)(1) of the Social Security Act. The purpose of these provisions is to promote administrative simplification.

§ 160.102 Applicability.

Except as otherwise provided, the standards, requirements, and implementation specifications adopted or designated under the parts of this subchapter apply to any entity that is:

(a) A health plan;

(b) A health care clearinghouse; and

(c) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

§ 160.103 Definitions.

Except as otherwise provided, the following definitions apply to this subchapter:

Act means the Social Security Act, as amended.

Covered entity means an entity described in § 160.102.

Health care means the provision of care, services, or supplies to a patient and includes any:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure with respect to the physical or mental condition, or functional status, of a patient or affecting the structure or function of the body;

(2) Sale or dispensing of a drug, device, equipment, or other item pursuant to a prescription; or

(3) Procurement or banking of blood, sperm, organs, or any other tissue for administration to patients.

Health care clearinghouse means a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. The entity receives health care transactions from health care providers or other entities, translates the data from a given format into one acceptable to the intended payer or payers, and forwards the processed transaction to appropriate payers and clearinghouses. Billing services, repricing companies, community health management information systems, community health information systems, and ''value-added'' networks and switches are considered to be health care clearinghouses for purposes of this part, if they perform the functions of health care clearinghouses as described in the preceding sentences.

Health care provider means a provider of services as defined in section 1861(u) of the Act, a provider of medical or health services as defined in section 1861(s) of the Act, and any other person or organization who furnishes, bills, or is paid for health care services or supplies in the normal course of business.

Health information means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Health plan means an individual or group plan that provides, or pays the cost of, medical care. Such term includes, when applied to government funded or assisted programs, the components of the government agency administering the program. ''Health plan'' includes the following, singly or in combination:

(1) A group health plan, defined as an employee welfare benefit plan (as currently defined in section 3(1) of the Employee Retirement Income and Security Act of 1974, 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg–91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance or otherwise, that:

(i) Has 50 or more participants; or

(ii) Is administered by an entity other than the employer that established and maintains the plan.

(2) A health insurance issuer, defined as an insurance company, insurance service, or insurance organization that is licensed to engage in the business of insurance in a State and is subject to State or other law that regulates insurance.

(3) A health maintenance organization, defined as a federally qualified health maintenance organization, an organization recognized as a health maintenance organization under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such a health maintenance organization.

(4) Part A or Part B of the Medicare program under title XVIII of the Act.

(5) The Medicaid program under title XIX of the Act.

(6) A Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss).

(7) A long-term care policy, including a nursing home fixed-indemnity policy.

(8) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(9) The health care program for active military personnel under title 10 of the United States Code.

(10) The veterans health care program under 38 U.S.C. chapter 17.

(11) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), as defined in 10 U.S.C. 1072(4).

(12) The Indian Health Service program under the Indian Health Care Improvement Act (25 U.S.C. 1601, *et seq.*).

(13) The Federal Employees Health Benefits Program under 5 U.S.C. chapter 89.

(14) An approved State child health plan for child health assistance that meets the requirements of section 2103 of the Act.

(15) A Medicare Plus Choice organization as defined in 42 CFR 422.2, with a contract under 42 CFR part 422, subpart K.

(16) Any other individual or group health plan, or combination thereof, that provides or pays for the cost of medical care.

Secretary means the Secretary of Health and Human Services and any other officer or employee of the Department of Health and Human Services to whom the authority involved has been delegated.

Small health plan means a health plan with annual receipts of $5 million or less.

Standard means a prescribed set of rules, conditions, or requirements concerning classification of components, specification of materials, performance or operations, or delineation of procedures, in describing products, systems, services or practices.

State includes the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

Transaction means the exchange of information between two parties to carry out financial or administrative activities related to health care. It includes the following:

(1) Health claims or equivalent encounter information;

(2) Health care payment and remittance advice;

(3) Coordination of benefits;

(4) Health claims status;

(5) Enrollment and disenrollment in a health plan;

(6) Eligibility for a health plan;

(7) Health plan premium payments;

(8) Referral certification and authorization;

(9) First report of injury;

(10) Health claims attachments; and

(11) Other transactions as the Secretary may prescribe by regulation.

§ 160.104 Effective dates of a modification to a standard or implementation specification.

The Secretary may modify a standard or implementation specification after the first year in which the standard or implementation specification is required to be used, but not more frequently than once every 12 months. If the Secretary adopts a modification to a standard or implementation specification, the implementation date of the modified standard or implementation specification may be no earlier than 180 days following the adoption of the modification. The Secretary will determine the actual date, taking into account the time needed to comply due to the nature and extent of the modification. The Secretary may extend the time for compliance for small health plans.

Subpart B—Preemption of State Law

§ 160.201 Applicability.

The provisions of this subpart apply to determinations and advisory opinions issued by the Secretary pursuant to 42 U.S.C. 1320d–7.

§ 160.202 Definitions.

For the purpose of this subpart, the following terms have the following meanings:

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

(1) A party would find it impossible to comply with both the State and federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104–191, as applicable.

More stringent means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a law which meets one or more of the following criteria, as applicable:

(1) With respect to a use or disclosure, provides a more limited use or disclosure (in terms of the number of potential recipients of the information, the amount of information to be disclosed, or the circumstances under which information may be disclosed).

(2) With respect to the rights of individuals of access to or amendment of individually identifiable health information, permits greater rights or access or amendment, as applicable, provided, however, that nothing in this subchapter shall be construed to preempt any State law to the extent that it authorizes or prohibits disclosure of protected health information regarding a minor to a parent, guardian or person acting *in loco parentis* of such minor.

(3) With respect to penalties, provides greater penalties.

(4) With respect to information to be provided to an individual about a proposed use, disclosure, rights, remedies, and similar issues, provides the greater amount of information.

(5) With respect to form or substance of authorizations for use or disclosure of information, provides requirements that narrow the scope or duration, increase the difficulty of obtaining, or reduce the coercive effect of the circumstances surrounding the authorization.

(6) With respect to recordkeeping or accounting requirements, provides for the retention or reporting of more detailed information or for a longer duration.

(7) With respect to any other matter, provides greater privacy protection for the individual.

Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or the effect of affecting the privacy of health information in a direct, clear, and substantial way.

State law means a law, decision, rule, regulation, or other State action having the effect of law.

§ 160.203 General rule and exceptions.

General rule. A standard, requirement, or implementation specification adopted under or pursuant to this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except where one or more of the following conditions is met:

(a) A determination is made by the Secretary pursuant to § 160.204(a) that the provision of State law:

(1) Is necessary:

(i) To prevent fraud and abuse;

(ii) To ensure appropriate State regulation of insurance and health plans;

(iii) For State reporting on health care delivery or costs; or

(iv) For other purposes related to improving the Medicare program, the Medicaid program, or the efficiency and effectiveness of the health care system; or

(2) Addresses controlled substances.

(b) The provision of State law relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

(c) The provision of State law, or the State established procedures, are established under a State law providing for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification.

§ 160.204 Process for requesting exception determinations or advisory opinions.

(a) *Determinations.* (1) A State may submit a written request to the Secretary to except a provision of State law from preemption under § 160.203(a). The request must include the following information:

(i) The State law for which the exception is requested;

(ii) The particular standard(s), requirement(s), or implementation specification(s) for which the exception is requested;

(iii) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;

(iv) How health care providers, health plans, and other entities would be affected by the exception;

(v) The length of time for which the exception would be in effect, if less than three years;

(vi) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and

(vii) Any other information the Secretary may request in order to make the determination.

(2) Requests for exception under this section must be submitted to the Secretary at an address which will be published in the **Federal Register**. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.

(3) The Secretary's determination under this paragraph will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met. If it is determined that the federal standard, requirement, or implementation specification accomplishes the purposes of the criterion or criteria at § 160.203(a) as well as or better than the State law for which the request is made, the request will be denied.

(4) An exception granted under this paragraph is effective for three years or for such lesser time as is specified in the determination granting the request.

(5) If an exception is granted under this paragraph, the exception has effect only with respect to transactions taking place wholly within the State for which the exception was requested.

(6) Any change to the standard, requirement, or implementation specification or provision of State law upon which an exception was granted requires a new request for an exception. Absent such a request and a favorable determination thereon, the standard, requirement, or implementation specification remains in effect. The responsibility for recognizing the need for and making the request lies with the original requestor.

(7) The Secretary may seek changes to a standard, requirement, or implementation specification based on requested exceptions or may urge the requesting State or other organizations or persons to do so.

(8) Determinations made by the Secretary pursuant to this paragraph will be published annually in the **Federal Register**.

(b) *Advisory opinions.*—(1) The Secretary may issue advisory opinions as to whether a provision of State law constitutes an exception under § 160.203(b) to the general rule of preemption under that section. The Secretary may issue such opinions at the request of a State or at the Secretary's own initiative.

(2) A State may submit a written request to the Secretary for an advisory opinion under this paragraph. The

request must include the following information:

(i) The State law for which the exception is requested;

(ii) The particular standard(s), requirement(s), or implementation specification(s) for which the exception is requested;

(iii) How health care providers, health plans, and other entities would be affected by the exception;

(iv) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets the criteria at § 160.203(b); and

(v) Any other information the Secretary may request in order to issue the advisory opinion.

(3) The requirements of paragraphs (a)(2), (a)(5)–(a)(7) of this section apply to requests for advisory opinions under this paragraph.

(4) The Secretary's decision under this paragraph will be made on the basis of the extent to which the information provided and other factors demonstrate that the criteria at § 160.203(b) are met.

(5) Advisory opinions made by the Secretary pursuant to this paragraph will be published annually in the **Federal Register**.

PARTS 161–163—[RESERVED]

PART 164—SECURITY AND PRIVACY

Subpart A—General Provisions

Subparts B–D—[Reserved]

Subpart E—Privacy of Individually Identifiable Health Information

Authority: 42 U.S.C. 1320d–2 and 1320d–4.

Subpart A—General Provisions

§ 164.102 Statutory basis.

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

§ 164.104 Applicability.

Except as otherwise provided, the provisions of this part apply to covered entities: health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction referred to in section 1173(a)(1) of the Act.

Subpart B–D—[Reserved]

Subpart E—Privacy of Individually Identifiable Health Information

§ 164.502 Applicability.

In addition to the applicable provisions of part 160 of this subchapter and except as otherwise herein provided, the requirements, standards, and implementation specifications of this subpart apply to covered entities with respect to protected health information.

§ 164.504 Definitions.

As used in this subpart, the following terms have the following meanings:

Business partner means, with respect to a covered entity, a person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. ''Business partner'' includes contractors or other persons who receive protected health information from the covered entity (or from another business partner of the covered entity) for the purposes described in the previous sentence, including lawyers, auditors, consultants, third-party administrators, health care clearinghouses, data processing firms, billing firms, and other covered entities. ''Business partner'' excludes persons who are within the covered entity's workforce, as defined in this section.

Designated record set means a group of records under the control of a 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 and which is used by the covered entity to make decisions about the individual. For purposes of this paragraph, the term *record* means any item, collection, or grouping of protected health information maintained, collected, used, or disseminated by a covered entity.

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

Health care operations means the following activities undertaken by or on behalf of a covered entity that is a health plan or health care provider for the purpose of carrying out the management functions of such entity necessary for the support of treatment or payment:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which undergraduate and graduate students and trainees in areas of health care learn under supervision to practice as health care providers, accreditation, certification, licensing or credentialing activities;

(3) Insurance rating and other insurance activities relating to the renewal of a contract for insurance, including underwriting, experience rating, and reinsurance, but only when the individuals are already enrolled in the health plan conducting such activities and the use or disclosure of protected health information relates to an existing contract of insurance (including the renewal of such a contract);

(4) Conducting or arranging for medical review and auditing services, including fraud and abuse detection and compliance programs; and

(5) Compiling and analyzing information in anticipation of or for use in a civil or criminal legal proceeding.

Health oversight agency means an agency, person or entity, including the employees or agents thereof,

(1) That is:

(i) A public agency; or

(ii) A person or entity acting under grant of authority from or contract with a public agency; and

(2) Which performs or oversees the performance of any audit; investigation; inspection; licensure or discipline; civil, criminal, or administrative proceeding or action; or other activity necessary for appropriate oversight of the health care system, of government benefit programs for which health information is relevant to beneficiary eligibility, or of government regulatory programs for which health information is necessary

for determining compliance with program standards.

Individual means the person who is the subject of protected health information, except that:

(1) ''Individual'' includes:

(i) With respect to adults and emancipated minors, legal representatives (such as court-appointed guardians or persons with a power of attorney), to the extent to which applicable law permits such legal representatives to exercise the person's rights in such contexts.

(ii) With respect to unemancipated minors, a parent, guardian, or person acting *in loco parentis*, provided that when a minor lawfully obtains a health care service without the consent of or notification to a parent, guardian, or other person acting *in loco parentis*, the minor shall have the exclusive right to exercise the rights of an individual under this subpart with respect to the protected health information relating to such care.

(iii) With respect to deceased persons, an executor, administrator, or other person authorized under applicable law to act on behalf of the decedent's estate.

(2) ''Individual'' excludes:

(i) Foreign military and diplomatic personnel and their dependents who receive health care provided by or paid for by the Department of Defense or other federal agency, or by an entity acting on its behalf, pursuant to a country-to-country agreement or federal statute; and

(ii) Overseas foreign national beneficiaries of health care provided by the Department of Defense or other federal agency, or by a non-governmental organization acting on its behalf.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and that:

(1) Is created by or received from a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and

(i) Which identifies the individual, or

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

Law enforcement official means an officer of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to conduct:

(1) An investigation or official proceeding inquiring into a violation of, or failure to comply with, any law; or

(2) A criminal, civil, or administrative proceeding arising from a violation of, or failure to comply with, any law.

Payment means:

(1) The activities undertaken by or on behalf of a covered entity that is:

(i) A health plan, or by a business partner on behalf of a health plan, to obtain premiums or to determine or fulfill its responsibility for coverage under the health plan and for provision of benefits under the health plan; or

(ii) A health care provider or health plan, or a business partner on behalf of such provider or plan, to obtain reimbursement for the provision of health care.

(2) Activities that constitute payment include:

(i) Determinations of coverage, improving methods of paying or coverage policies, adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, and medical data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and

(v) Utilization review activities, including precertification and preauthorization of services.

Protected health information means individually identifiable health information that is or has been electronically transmitted or electronically maintained by a covered entity and includes such information in any other form.

(1) For purposes of this definition,

(i) ''Electronically transmitted'' includes information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmissions over the Internet, Extranet, leased lines, dial-up lines, private networks, telephone voice response, and ''faxback'' systems.

(ii) ''Electronically maintained'' means information stored by a computer or on any electronic medium from which information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

(2) ''Protected health information'' excludes:

(i) Individually identifiable health information in education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and

(ii) Individually identifiable health information of inmates of correctional facilities and detainees in detention facilities.

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe that is responsible for public health matters as part of its official mandate.

Research means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. ''Generalizable knowledge'' is knowledge related to health that can be applied to populations outside of the population served by the covered entity.

Treatment means the provision of health care by, or the coordination of health care (including health care management of the individual through risk assessment, case management, and disease management) among, health care providers; the referral of a patient from one provider to another; or the coordination of health care or other services among health care providers and third parties authorized by the health plan or the individual.

Use means the employment, application, utilization, examination, or analysis of information within an entity that holds the information.

Workforce means employees, volunteers, trainees, and other persons under the direct control of a covered entity, including persons providing labor on an unpaid basis.

§ 164.506 Uses and disclosures of protected health information: general rules.

(a) *Standard.* A covered entity may not use or disclose an individual's protected health information, except as otherwise permitted or required by this part or as required to comply with applicable requirements of this subchapter.

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

(i) Except for research information unrelated to treatment, to carry out treatment, payment, or health care operations;

(ii) Pursuant to an authorization by the individual that complies with § 164.508; or

(iii) As permitted by and in compliance with this section or § 164.510.

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

(i) To an individual, when a request is made under § 164.514; or

(ii) When required by the Secretary under § 164.522 to investigate or determine the entity's compliance with this part.

(b)(1) *Standard: Minimum necessary.* A covered entity must make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose of the use or disclosure. This requirement does not apply to uses or disclosures that are:

(i) Made in accordance with §§ 164.508(a)(1), 164.514, or § 164.522;

(ii) Required by law and permitted under § 164.510;

(iii) Required for compliance with applicable requirements of this subchapter; or

(iv) Made by a covered health care provider to a covered health plan, when the information is requested for audit and related purposes.

(2) *Implementation specification: Procedures.* To comply with the standard in this paragraph, a covered entity must have procedures to:

(i) Identify appropriate persons within the entity to determine what information should be used or disclosed consistent with the minimum necessary standard;

(ii) Ensure that the persons identified under paragraph (b)(2)(i) of this section make the minimum necessary determinations, when required;

(iii) Within the limits of the entity's technological capabilities, provide for the making of such determinations individually.

(3) *Implementation specification: Reliance.* When making disclosures to public officials that are permitted under § 164.510 but not required by other law, a covered entity may reasonably rely on the representations of such officials that the information requested is the minimum necessary for the stated purpose(s).

(c)(1) *Standard: Right of an individual to restrict uses and disclosures.* (i) A covered entity that is a health care provider must permit individuals to request that uses or disclosures of protected health information for treatment, payment, or health care operations be restricted, and, if the requested restrictions are agreed to by the provider, not make uses or disclosures inconsistent with such restrictions.

(ii) This requirement does not apply:

(A) To uses or disclosures permitted under § 164.510;

(B) When the health care services provided are emergency services or the information is requested pursuant to § 164.510(k) and

(C) To disclosures to the Secretary pursuant to § 164.522.

(iii) A provider is not required to agree to a requested restriction.

(2) *Implementation specifications.* A covered entity must have procedures that:

(i) Provide individuals an opportunity to request a restriction on the uses and disclosures of their protected health information;

(ii) Provide that restrictions that are agreed to by the entity are reduced to writing or otherwise documented;

(iii) Enable the entity to honor such restrictions; and

(iv) Provide for the notification of others to whom such information is disclosed of such restriction.

(d)(1) *Standard: use or disclosure of de-identified protected health information.* The requirements of this subpart do not apply to protected health information that a covered entity has de-identified, provided, however, that:

(i) Disclosure of a key or other device designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If a covered entity re-identifies de-identified information, it may use or disclose such re-identified information only in accordance with this subpart.

(2) *Implementation specifications.* (i) A covered entity may use protected health information to create de-identified information by removing, coding, encrypting, or otherwise eliminating or concealing the information that makes such information individually identifiable.

(ii) Information is presumed not to be individually identifiable (de-identified), if:

(A) The following identifiers have been removed or otherwise concealed:

(*1*) Name;

(*2*) Address, including street address, city, county, zip code, and equivalent geocodes;

(*3*) Names of relatives;

(*4*) Name of employers;

(*5*) Birth date;

(*6*) Telephone numbers;

(*7*) Fax numbers;

(*8*) Electronic mail addresses;

(*9*) Social security number;

(*10*) Medical record number;

(*11*) Health plan beneficiary number;

(*12*) Account number;

(*13*) Certificate/license number;

(*14*) Any vehicle or other device serial number;

(*15*) Web Universal Resource Locator (URL);

(*16*) Internet Protocol (IP) address number;

(*17*) Finger or voice prints;

(*18*) Photographic images; and

(*19*) Any other unique identifying number, characteristic, or code that the covered entity has reason to believe may be available to an anticipated recipient of the information; and

(B) The covered entity has no reason to believe that any anticipated recipient of such information could use the information, alone or in combination with other information, to identify an individual.

(iii) Notwithstanding paragraph (d)(2)(ii) of this section, entities with appropriate statistical experience and expertise may treat information as de-identified, if they include information listed in paragraph (d)(2)(ii) of this section and they determine that the probability of identifying individuals with such identifying information retained is very low, or may remove additional information, if they have a reasonable basis to believe such additional information could be used to identify an individual.

(e)(1) *Standards: Business partners.* (i) Except for disclosures of protected health information by a covered entity that is a health care provider to another health care provider for consultation or referral purposes, a covered entity may not disclose protected health information to a business partner without satisfactory assurance from the business partner that it will appropriately safeguard the information.

(ii) A covered entity must take reasonable steps to ensure that each business partner complies with the requirements of this subpart with respect to any task or other activity it performs on behalf of the entity, to the extent the covered entity would be required to comply with such requirements.

(2) *Implementation specifications.* (i) For the purposes of this section, *satisfactory assurance* means a contract between the covered entity and the business partner to which such information is to be disclosed that establishes the permitted and required uses and disclosures of such information by the partner. The contract must provide that the business partner will:

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

(B) Not use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;

(C) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;

(D) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;

(E) Ensure that any subcontractors or agents to whom it provides protected health information received from the covered entity agree to the same restrictions and conditions that apply to the business partner with respect to such information;

(F) Make available protected health information in accordance with § 164.514(a);

(G) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart;

(H) At termination of the contract, return or destroy all protected health information received from the covered entity that the business partner still maintains in any form and retain no copies of such information; and

(I) Incorporate any amendments or corrections to protected health information when notified pursuant to § 164.516(c)(3).

(ii) The contract required by paragraph (e)(2)(i) of this section must:

(A) State that the individuals whose protected health information is disclosed under the contract are intended third party beneficiaries of the contract; and

(B) Authorize the covered entity to terminate the contract, if the covered entity determines that the business partner has violated a material term of the contract required by this paragraph.

(iii) A material breach by a business partner of its obligations under the contract required by paragraph (e)(2)(i) of this section will be considered to be noncompliance of the covered entity with the applicable requirements of this subpart, if the covered entity knew or reasonably should have known of such breach and failed to take reasonable steps to cure the breach or terminate the contract.

(f) *Standard: Deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for two years following the death of such individual. This requirement does not apply to uses or disclosures for research purposes.

(g) *Standard: uses and disclosures consistent with notice.* Except as provided by § 164.520(g)(2), a covered entity that is required by § 164.512 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice.

§ 164.508 Uses and disclosures for which individual authorization is required.

(a) *Standard.* An authorization executed in accordance with this section is required in order for the covered entity to use or disclose protected health information in the following situations:

(1) *Request by individual.* Where the individual requests the covered entity to use or disclose the information.

(2) *Request by covered entity.* (i) Where the covered entity requests the individual to authorize the use or disclosure of the information. The covered entity must request and obtain an authorization from the individual for all uses and disclosures that are not:

(A) Except as provided in paragraph (a)(3) of this section, compatible with or directly related to treatment, payment, or health care operations;

(B) Covered by § 164.510;

(C) Covered by paragraph (a)(1) of this section; or

(D) Required by this subpart.

(ii) Uses and disclosures of protected health information for which individual authorization is required include, but are not limited to, the following:

(A) Use for marketing of health and non-health items and services by the covered entity;

(B) Disclosure by sale, rental, or barter;

(C) Use and disclosure to non-health related divisions of the covered entity, e.g., for use in marketing life or casualty insurance or banking services;

(D) Disclosure, prior to an individual's enrollment in a health plan, to the health plan or health care provider for making eligibility or enrollment determinations relating to the individual or for underwriting or risk rating determinations;

(E) Disclosure to an employer for use in employment determinations; and

(F) Use or disclosure for fundraising purposes.

(iii) A covered entity may not condition the provision to an individual of treatment or payment on the provision by the individual of a requested authorization for use or disclosure, except where the authorization is requested in connection with a clinical trial.

(iv) Except where required by law, a covered entity may not require an individual to sign an authorization for use or disclosure of protected health information for treatment, payment, or health care operations purposes.

(3) *Authorization required: Special cases.* (i) Except as otherwise required by this subpart or permitted under § 164.510, a covered entity must obtain the authorization of the individual for the following uses and disclosures of protected health information about the individual:

(A) Use by a person other than the creator, or disclosure, of psychotherapy notes; and

(B) Use or disclosure of research information unrelated to treatment.

(ii) The requirements of paragraphs (b) through (e) of this section apply to such authorizations, as appropriate.

(iii) A covered entity may not condition treatment, enrollment in a health plan, or payment on a requirement that the individual authorize use or disclosure of psychotherapy notes relating to the individual.

(iv) For purposes of this section:

(A) *Psychotherapy notes* means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session. For purposes of this definition, ''psychotherapy notes'' excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis and progress to date.

(B) *Research information unrelated to treatment* means health information that is received or created by a covered entity in the course of conducting research, for which there is insufficient scientific and medical evidence regarding the validity or utility of the information such that it should not be used for the purpose of providing health care, and with respect to which the covered entity has not requested payment from a third party payor.

(b) *General implementation specifications for authorizations.*—(1) *General requirements.* A copy of the model form which appears in Appendix A hereto, or a document that contains the elements listed in paragraphs (c) or (d) of this section, as applicable, must be accepted by the covered entity.

(2) *Defective authorizations.* There is no ''authorization'' within the meaning of this section, if the submitted form has any of the following defects:

(i) The expiration date has passed;

(ii) The form has not been filled out completely;

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The form lacks an element required by paragraph (c) or (d) of this section, as applicable;

(v) The information on the form is known by the covered entity to be false.

(3) *Compound authorizations.* Except where authorization is requested in connection with a clinical trial, an authorization for use or disclosure of protected health information for purposes other than treatment or payment may not be in the same document as an authorization for or consent to treatment or payment.

(c) *Implementation specifications for authorizations requested by an individual.*—(1) *Required elements.* Before a covered entity may use or disclose protected health information of an individual pursuant to a request from the individual, it must obtain a completed authorization for use or disclosure executed by the individual that contains at least the following elements:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

(ii) The name of the covered entity, or class of entities or persons, authorized to make the requested use or disclosure;

(iii) The name or other specific identification of the person(s) or entity(ies), which may include the covered entity itself, to whom the covered entity may make the requested use or disclosure;

(iv) An expiration date;

(v) Signature and date;

(vi) If the authorization is executed by a legal representative or other person authorized to act for the individual, a description of his or her authority to act or relationship to the individual;

(vii) A statement in which the individual acknowledges that he or she has the right to revoke the authorization, except to the extent that information has already been released under the authorization; and

(viii) A statement in which the individual acknowledges that information used or disclosed to any entity other than a health plan or health care provider may no longer be protected by the federal privacy law.

(2) *Plain language requirement.* The model form at appendix A to this subpart may be used. If the model form at appendix A to this subpart is not used, the authorization form must be written in plain language.

(d) *Implementation specifications for authorizations for uses and disclosures requested by covered entities.*—(1) *Required elements.* Before a covered entity may use or disclose protected health information of an individual pursuant to a request that it has made, it must obtain a completed authorization for use or disclosure executed by the individual that meets the requirements of paragraph (c) of this section and contains the following additional elements:

(i) Except where the authorization is requested for a clinical trial, a statement that it will not condition treatment or payment on the individual's providing authorization for the requested use or disclosure;

(ii) A description of the purpose(s) of the requested use or disclosure;

(iii) A statement that the individual may:

(A) Inspect or copy the protected health information to be used or disclosed as provided in § 164.514; and

(B) Refuse to sign the authorization; and

(iv) Where use or disclosure of the requested information will result in financial gain to the entity, a statement that such gain will result.

(2) *Required procedures.* In requesting authorization from an individual under this paragraph, a covered entity must:

(i) Have procedures designed to enable it to request only the minimum amount of protected health information necessary to accomplish the purpose for which the request is made; and

(ii) Provide the individual with a copy of the executed authorization.

(e) *Revocation of authorizations.* An individual may revoke an authorization to use or disclose his or her protected health information at any time, except to the extent that the covered entity has taken action in reliance thereon.

§ 164.510 Uses and disclosures for which individual authorization is not required.

A covered entity may use or disclose protected health information, for purposes other than treatment, payment, or health care operations, without the authorization of the individual, in the situations covered by this section and subject to the applicable requirements provided for by this section.

(a) *General requirements.* In using or disclosing protected health information under this section:

(1) *Verification.* A covered entity must comply with any applicable verification requirements under § 164.518(c).

(2) *Health care clearinghouses.* A health care clearinghouse that uses or discloses protected health information it maintains as a business partner of a covered entity may not make uses or disclosures otherwise permitted under this section that are not permitted by the terms of its contract with the covered entity under § 164.506(e).

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

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions;

(ii) A public health authority or other appropriate authority authorized by law to receive reports of child abuse or neglect;

(iii) A person or entity other than a governmental authority that can demonstrate or demonstrates that it is acting to comply with requirements or direction of a public health authority; or

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition and is authorized by law to be notified as necessary in the conduct of a public health intervention or investigation.

(2) *Permitted use.* Where the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) *Disclosures and uses for health oversight activities.*—(1) *Permitted disclosures.* A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audit, investigation, inspection, civil, criminal, or administrative proceeding or action, or other activity necessary for appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility; or

(iii) Government regulatory programs for which health information is necessary for determining compliance with program standards.

(2) *Permitted use.* Where a covered entity is itself a health oversight agency, the covered entity may use protected health information for health oversight activities described by paragraph (c)(1) of this section.

(d) *Disclosures and uses for judicial and administrative proceedings.*—(1) *Permitted disclosures.* A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal; or

(ii) Where the individual is a party to the proceeding and his or her medical condition or history is at issue and the disclosure is pursuant to lawful process or otherwise authorized by law.

(2) *Permitted use.* Where the covered entity is itself a government agency, the covered entity may use protected health information in all cases in which it is permitted to disclose such information in the course of any judicial or administrative proceeding under paragraph (d)(1) of this section.

(3) *Additional restriction.* (i) Where the request for disclosure of protected health information is accompanied by a court order, the covered entity may disclose only that protected health information which the court order authorizes to be disclosed.

(ii) Where the request for disclosure of protected health information is not accompanied by a court order, the covered entity may not disclose the information requested unless a request authorized by law has been made by the agency requesting the information or by legal counsel representing a party to litigation, with a written statement certifying that the protected health information requested concerns a litigant to the proceeding and that the health condition of such litigant is at issue at such proceeding.

(e) *Disclosures to coroners and medical examiners.* A covered entity may disclose protected health information to a coroner or medical examiner, consistent with applicable law, for the purposes of identifying a deceased person or determining a cause of death.

(f) *Disclosures for law enforcement purposes.* A covered entity may disclose protected health information to a law enforcement official if:

(1) *Pursuant to process.* (i) The law enforcement official is conducting or supervising a law enforcement inquiry or proceeding authorized by law and the disclosure is:

(A) Pursuant to a warrant, subpoena, or order issued by a judicial officer that documents a finding by the judicial officer;

(B) Pursuant to a grand jury subpoena; or

(C) Pursuant to an administrative request, including an administrative subpoena or summons, a civil investigative demand, or similar process authorized under law, provided that:

(*1*) The information sought is relevant and material to a legitimate law enforcement inquiry;

(*2*) The request is as specific and narrowly drawn as is reasonably practicable; and

(*3*) De-identified information could not reasonably be used.

(ii) For the purposes of this paragraph, ''law enforcement inquiry or proceeding'' means:

(A) An investigation or official proceeding inquiring into a violation of, or failure to comply with, law; or

(B) A criminal, civil, or administrative proceeding arising from a violation of, or failure to comply with, law.

(2) *Limited information for identifying purposes.* The disclosure is for the purpose of identifying a suspect, fugitive, material witness, or missing person, *provided* that, the covered entity may disclose only the following information:

(i) Name;

(ii) Address;

(iii) Social security number;

(iv) Date of birth;

(v) Place of birth;

(vi) Type of injury or other distinguishing characteristic; and

(vii) Date and time of treatment.

(3) *Information about a victim of crime or abuse.* The disclosure is of the protected health information of an individual who is or is suspected to be a victim of a crime, abuse, or other harm, if the law enforcement official represents that:

(i) Such information is needed to determine whether a violation of law by a person other than the victim has occurred; and

(ii) Immediate law enforcement activity that depends upon obtaining such information may be necessary.

(4) *Intelligence and national security activities.* The disclosure is:

(i) For the conduct of lawful intelligence activities conducted pursuant to the National Security Act (50 U.S.C. 401, *et seq.*);

(ii) Made in connection with providing protective services to the President or other persons pursuant to 18 U.S.C. 3056; or

(iii) Made pursuant to 22 U.S.C. 2709(a)(3).

(5) *Health care fraud.* The covered entity believes in good faith that the information disclosed constitutes evidence of criminal conduct:

(i) That arises out of and is directly related to:

(A) The receipt of health care or payment for health care, including a fraudulent claim for health care;

(B) Qualification for or receipt of benefits, payments, or services based on a fraudulent statement or material misrepresentation of the health of the individual;

(ii) That occurred on the premises of the covered entity; or

(iii) Was witnessed by a member of the covered entity's workforce.

(5) *Urgent circumstances.* The disclosure is of the protected health information of an individual who is or is suspected to be a victim of a crime, abuse, or other harm, if the law enforcement official represents that:

(i) Such information is needed to determine whether a violation of law by a person other than the victim has occurred; and

(ii) Immediate law enforcement activity that depends upon obtaining such information may be necessary.

(g) *Disclosures and uses for governmental health data systems.*—(1) *Permitted disclosures.* A covered entity may disclose protected health information to a government agency, or private entity acting on behalf of a government agency, for inclusion in a governmental health data system that collects health data for analysis in support of policy, planning, regulatory, or management functions authorized by law.

(2) *Permitted uses.* Where a covered entity is itself a government agency that collects health data for analysis in support of policy, planning, regulatory, or management functions, the covered entity may use protected health information in all cases in which it is permitted to disclose such information for government health data systems under paragraph (g)(1) of this section.

(h) *Disclosures of directory information.* (1) *Individuals with capacity.* For individuals with the capacity to make their own health care decisions, a covered entity that is a health care provider may disclose protected health information for directory purposes, provided that, the individual has agreed to such disclosure.

(2) *Incapacitated individuals.* For individuals who are incapacitated, a covered entity that is a health care provider may, at its discretion and consistent with good medical practice and any prior expressions of preference of which the covered entity is aware, disclose protected health information for directory purposes.

(3) *Information to be disclosed.* The information that may be disclosed for directory purposes pursuant to paragraphs (h)(1) and (2) of this section, is limited to:

(i) Name of the individual;

(ii) Location of the individual in the health care provider's facility; and

(iii) Description of the individual's condition in general terms that do not communicate specific medical information about the individual.

(i) *Disclosures for banking and payment processes.* A covered entity may disclose, in connection with routine banking activities or payment by debit, credit, or other payment card, or other payment means, the minimum amount of protected health information necessary to complete a banking or payment activity to:

(1) *Financial institutions.* An entity engaged in the activities of a financial institution (as defined in section 1101 of the Right to Financial Privacy Act of 1978); or

(2) *Entities acting on behalf of financial institutions.* An entity engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for an entity described in paragraph (i)(1) of this section.

(j) *Uses and disclosures for research purposes.* A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that, the covered entity has obtained written documentation of the following:

(1) *Waiver of authorization.* A waiver, in whole or in part, of authorization for use or disclosure of protected health information that has been approved by either:

(i) An Institutional Review Board, established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 28 CFR 46.107.32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107.45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(ii) A privacy board that:

(A) Has members with varying backgrounds and appropriate professional competency as necessary to review the research protocol;

(B) Includes at least one member who is not affiliated with the entity conducting the research or related to a person who is affiliated with such entity; and

(C) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(2) *Date of approval.* The date of approval of the waiver, in whole or in part, of authorization by an Institutional Review Board or privacy board.

(3) *Criteria.* The Institutional Review Board or privacy board has determined that the waiver, in whole or in part, of authorization satisfies the following criteria:

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

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

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

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

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

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

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

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

(4) *Required signature.* The written documentation must be signed by the chair of, as applicable, the Institutional Review Board or the privacy board.

(k) *Uses and disclosures in emergency circumstances.*—(1) *Permitted disclosures.* A covered entity may, consistent with applicable law and standards of ethical conduct and 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 an individual or the public, use or disclose protected health information to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

(2) *Presumption of reasonable belief.* A covered entity that makes a disclosure pursuant to paragraph (k)(1) of this section is presumed to have acted under a reasonable belief, if the disclosure is made in good faith based upon a credible representation by a person with apparent knowledge or authority (such as a doctor or law enforcement or other government official).

(l) *Disclosures to next-of-kin.*—(1) *Permitted disclosures.* A covered entity may disclose protected health information to a person who is a next-of-kin, other family member, or close personal friend of an individual who possesses the capacity to make his or her own health care decisions, if:

(i) The individual has verbally agreed to the disclosure; or

(ii) In circumstances where such agreement cannot practicably or reasonably be obtained, only the protected health information that is directly relevant to the person's involvement in the individual's health care is disclosed, consistent with good health professional practices and ethics.

(2) *Next-of-kin defined.* For purposes of this paragraph, ''next-of-kin'' is defined as defined under applicable law.

(m) *Uses and disclosures for specialized classes.*—(1) *Military purposes.* A covered entity that is a health care provider or health plan providing health care to individuals who are Armed Forces personnel may use and disclose protected health information for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, where the appropriate military authority has published by notice in the **Federal Register** the following information:

(i) Appropriate military command authorities;

(ii) The circumstances for which use or disclosure without individual authorization would be required; and

(iii) Activities for which such use or disclosure would occur in order to assure proper execution of the military mission.

(2) *Department of Veterans Affairs.* The Department of Veterans Affairs may use and disclose protected health information among components of the Department that determine eligibility for or entitlement to, or that provide, benefits under laws administered by the Secretary of Veterans Affairs.

(3) *Intelligence community.* A covered entity may disclose protected health information of an individual who is an employee of the intelligence community, as defined in section 4 of the National Security Act, 50 U.S.C. 401a, and his or her dependents, if such dependents are being considered for posting abroad, to intelligence community agencies, where authorized by law.

(4) *Department of State.* The Department of State may use protected health information about the following individuals for the following purposes:

(i) As to applicants to the Foreign Service, for medical clearance determinations about physical fitness to serve in the Foreign Service on a worldwide basis, including about medical and mental conditions limiting assignability abroad; determinations of conformance to occupational physical standards, where applicable; and determinations of suitability.

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

(iii) As to eligible family members of Foreign Service or other United States Government employees, for medical clearance determinations as described in paragraph (m)(4)(ii) of this section to permit eligible family members to accompany employees to posts abroad on Government orders; determinations regarding family members remaining at post; and separation medical examinations.

(n) *Uses and disclosures otherwise required by law.* A covered entity may use or disclose protected health information where such use or disclosure is required by law and the use or disclosure meets all relevant requirements of such law. This paragraph does not apply to uses or disclosures that are covered by paragraphs (b) through (m) of this section.

§ 164.512 Notice to individuals of information practices.

(a) *Standard.* An individual has a right to adequate notice of the policies and procedures of a covered entity that is a health plan or a health care provider with respect to protected health information.

(b) *Standard for notice procedures.* A covered entity that is a health plan or health care provider must have procedures that provide adequate notice to individuals of their rights and the procedures for exercising their rights under this subpart with respect to protected health information about them.

(c) *General implementation specification.* A covered entity that has and follows procedures that meet the requirements of this section will be presumed to have provided adequate notice under this section.

(d) *Implementation specifications: content of notice.*—(1) *Required elements.* Notices required to be provided under this section must include in plain language a statement of each of the following elements:

(i) *Uses and disclosures.* The uses and disclosures, and the entity's policies and procedures with respect to such uses and disclosures, must be described in sufficient detail to put the individual on notice of the uses and disclosures expected to be made of his or her protected health information. Such statement must:

(A) Describe the uses and disclosures that will be made without individual authorization; and

(B) Distinguish between those uses and disclosures the entity makes that are required by law and those that are permitted but not required by law.

(ii) *Required statements.* State that:

(A) Other uses and disclosures will be made only with the individual's authorization and that such authorization may be revoked;

(B) An individual may request that certain uses and disclosures of his or her protected health information be restricted, and the covered entity is not required to agree to such a request;

(C) An individual has the right to request, and a description of the procedures for exercising, the following with respect to his or her protected health information:

(*1*) Inspection and copying;

(*2*) Amendment or correction; and

(*3*) An accounting of the disclosures of such information by the covered entity;

(D) The covered entity is required by law to protect the privacy of its individually identifiable health information, provide a notice of its policies and procedures with respect to such information, and abide by the terms of the notice currently in effect;

(E) The entity may change its policies and procedures relating to protected health information at any time, with a description of how individuals will be informed of material changes; and

(F) Individuals may complain to the covered entity and to the Secretary if they believe that their privacy rights have been violated.

(iii) *Contact.* The name and telephone number of a contact person or office required by § 164.518(a)(2).

(iv) *Date.* The date the version of the notice was produced.

(2) *Revisions.* A covered health plan or health care provider may change its policies or procedures required by this subpart at any time. When a covered health plan or health care provider materially revises its policies and procedures, it must update its notice as provided for by § 164.520(g).

(e) *Implementation specifications: Provision of notice.* A covered entity must make the notice required by this section available:

(1) *General requirement.* On request; and

(2) *Specific requirements.* As follows:

(i) *Health plans.* Health plans must provide a copy of the notice to an individual covered by the plan:

(A) As of the date on which the health plan is required to be in compliance with this subpart;

(B) After the date described in paragraph (e)(2)(i)(A) of this section, at enrollment;

(C) After enrollment, within 60 days of a material revision to the content of the notice; and

(D) No less frequently than once every three years.

(ii) *Health care providers.* A health care provider must:

(A) During the one year period following the date by which the provider is required to come into compliance with this subpart, provide a copy to individuals currently served by the provider at the first service delivery to such individuals during such period, provided that, where service is not provided through a face-to-face contact, the provider must provide the notice in an appropriate manner within a reasonable period of time following first service delivery;

(B) After the one year period provided for by paragraph (e)(2)(ii)(A) of this section, provide a copy to individuals served by the provider at the first service delivery to such individuals, provided that, where service is not provided through a face-to-face contact, the provider must provide the notice in an appropriate manner within a reasonable period of time following first service delivery; and

(C) Post a copy of 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. Any revision to the notice must be posted promptly.

§ 164.514 Access of individuals to protected health information

(a) *Standard: Right of access.* An individual has a right of access to, which includes a right to inspect and obtain a copy of, his or her protected health information in designated record sets of a covered entity that is a health plan or a health care provider, including such information in a business partner's designated record set that is not a duplicate of the information held by the provider or plan, for so long as the information is maintained.

(b) *Standard: denial of access to protected health information.*—(1) *Grounds.* Except where the protected health information to which access is requested is subject to 5 U.S.C. 552a, a covered entity may deny a request for access under paragraph (a) of this section where:

(i) 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;

(ii) The information is about another person (other than a health care provider) and a licensed health care professional has determined that the inspection and copying requested is reasonably likely to cause substantial harm to such other person;

(iii) The 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;

(iv) The information was obtained by a covered entity that is a health care 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 clinical trial is in progress; or

(v) The information was compiled in reasonable anticipation of, or for use in, a legal proceeding.

(2) *Other information available.* Where a denial of protected health information is made pursuant to paragraph (b)(1) of this section, the covered entity must make any other protected health information requested available to the individual to the extent possible consistent with the denial.

(c) *Standard: procedures to protect rights of access.* A covered entity that is a health plan or a health care provider must have procedures that enable individuals to exercise their rights under paragraph (a) of this section.

(d) *Implementation specifications: Access to protected health information.* The procedures required by paragraph (c) of this section must:

(1) *Means of request.* Provide a means by which an individual can request inspection or a copy of protected health information about him or her.

(2) *Time limit.* Provide for taking action on such requests as soon as possible but not later than 30 days following receipt of the request.

(3) *Request accepted.* Where the request is accepted, provide:

(i) For notification of the individual of the decision and of any steps necessary to fulfill the request;

(ii) The information requested in the form or format requested, if it is readily producible in such form or format;

(iii) For facilitating the process of inspection and copying; and

(iv) For a reasonable, cost-based fee for copying health information provided pursuant to this paragraph, if deemed desirable by the entity.

(4) *Request denied.* Where the request is denied in whole or in part, provide the individual with a written statement in plain language of:

(i) The basis for the denial; and

(ii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.518(d)(2) or to the Secretary pursuant to the procedures established in § 164.522(b). The description must include:

(A) The name and telephone number of the contact person or office required by § 164.518(a)(2) of this subpart; and

(B) Information relevant to filing a complaint with the Secretary under § 164.522(b).

§ 164.515 Accounting for disclosures of protected health information.

(a) *Standard: Right to an accounting of disclosures of protected health information.* An individual has a right to receive an accounting of all disclosures of protected health information made by a covered entity as long as such information is maintained by the entity, except for disclosures:

(1) For treatment, payment and health care operations; and

(2) To health oversight or law enforcement agencies, if the health oversight or law enforcement agency has provided a written request stating that the exclusion is necessary because disclosure would be reasonably likely to impede the agency's activities and specifying the time for which such exclusion is required.

(b) *Standard: Procedures for accounting.* A covered entity must have procedures to give individuals an accurate accounting of disclosures for which an accounting is required by paragraph (a) of this section.

(c) *Implementation specifications: Accounting procedures.* The procedures required by paragraph (b) of this section must:

(1) Provide for an accounting of the following:

(i) The date of each disclosure;

(ii) The name and address of the organization or person who received the protected health information;

(iii) A brief description of the information disclosed;

(iv) For disclosures other than those made at the request of the individual, the purpose for which the information was disclosed; and (v) Provision of copies of all requests for disclosure.

(2) Provide the accounting to the individual as soon as possible, but no later than 30 days of receipt of the request therefor.

(3) Provide for a means of accounting for as long as the entity maintains the protected health information.

(4) Provide for a means of requiring business partners to provide such an accounting upon request of the covered entity.

§ 164.516 Amendment and correction.

(a) *Standard: right to request amendment or correction.*—(1) *Right to request.* An individual has the right to request a covered entity that is a health plan or health care provider to amend or correct protected health information about him or her in designated record sets of the covered entity for as long as the covered entity maintains the information.

(2) *Grounds for denial of request.* A covered entity may deny a request for amendment or correction of the individual's protected health information, if it determines that the information that is the subject of the request:

(i) Was not created by the covered entity;

(ii) Would not be available for inspection and copying under § 164.514 or

(iii) Is accurate and complete.

(b) *Standard: Amendment and correction procedures.* A covered entity that is a health plan or health care provider must have procedures to enable individuals to request amendment or correction, to determine whether the requests should be granted or denied, and to disseminate amendments or corrections to its business partners and others to whom erroneous information has been disclosed.

(c) *Implementation specifications: Procedures.* The procedures required by paragraph (b) of this section must provide that the covered entity will:

(1) *Means of request.* Provide a means by which an individual can request amendment or correction of his or her protected health information.

(2) *Time limit.* Take action on such request within 60 days of receipt of the request;

(3) *Request accepted.* Where the request is accepted in whole or in part:

(i) As otherwise required by this part, make the appropriate amendments or corrections;

(ii) As otherwise required by this part, identify the challenged entries as amended or corrected and indicate their location;

(iii) Make reasonable efforts to notify:

(A) Persons, organizations, or other entities the individual identifies as needing to be notified; and (B) Persons, organizations, or other entities, including business partners, who the covered entity knows have received the erroneous or incomplete information and who may have relied, or could foreseeably rely, on such information to the detriment of the individual; and (iv) Notify the individual of the decision to correct or amend the information.

(4) *Request denied.* Where the request is denied in whole or in part:

(i) Provide the individual with a written statement in plain language of:

(A) The basis for the denial;

(B) A description of how the individual may file a written statement of disagreement with the denial; and

(C) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.518(d) or to the Secretary pursuant to the procedures established in § 164.522(b). The description must include:

(*1*) The name and telephone number of the contact person or office required by § 164.518(a)(2); and

(*2*) Information relevant to filing a complaint with the Secretary under § 164.522(b).

(ii) The procedures of the covered entity must:

(A) Permit the individual to file a statement of the individual's disagreement with the denial and the basis of such disagreement.

(B) Provide for inclusion of the covered entity's statement of denial and the individual's statement of disagreement with any subsequent disclosure of the information to which the disagreement relates, provided, however, that the covered entity may establish a limit to the length of the statement of disagreement, and may summarize the statement of disagreement if necessary.

(C) Permit the covered entity to provide a rebuttal to the statement of disagreement in subsequent disclosures under paragraph (c)(4)(ii)(B) of this section.

(d) *Standard: Effectuating a notice of amendment or correction.* Any covered entity that receives a notice of amendment or correction must have procedures in place to make the amendment or correction in any of its designated record sets and to notify its business partners, as appropriate, of necessary amendments or corrections of protected health information.

(e) *Implementation specification: effectuating a notice of amendment or correction.* The procedures required by paragraph (d) of this section must specify the process for correction or amendment of information in all appropriate designated record sets maintained by the covered entity and its business partners.

§ 164.518 Administrative requirements.

Except as otherwise provided, a covered entity must meet the requirements of this section.

(a) *Designated privacy official: standard.*—(1) *Responsibilities of designated privacy official.* A covered entity must designate a privacy official who is responsible for the development and implementation of the privacy policies and procedures of the entity.

(2) *Contact person or office.* A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.512. If a covered entity designates a contact person, it may designate the privacy official as the contact person.

(b) *Training.*—(1) *Standard.* All members of the covered entity's workforce who, by virtue of their positions, are likely to obtain access to protected health information must receive training on the entity's policies and procedures required by this subpart that are relevant to carrying out their function within the entity.

(2) *Implementation specification.* A covered entity must train all members of its workforce who, by virtue of their positions, are likely to obtain access to protected health information. Such training must meet the following requirements:

(i) The training must occur:

(A) For members of the covered entity's workforce as of the date on which this subpart becomes applicable to such entity, by such date; and

(B) For persons joining the covered entity's workforce after the date in paragraph (b)(2)(i)(A) of this section, within a reasonable period after the person joins the workforce.

(ii) The covered entity must require members of its workforce trained as required by this section to sign, upon completing training, a certification. The certification must state:

(A) The date of training; and

(B) That the person completing the training will honor all of the entity's policies and procedures required by this subpart.

(iii) The covered entity must require members of its workforce trained as required by this section to sign, at least once every three years, a statement certifying that the person will honor all of the entity's policies and procedures required by this subpart.

(iv) The covered entity must provide all members of its workforce with access to protected health information within the entity with further training, as relevant to their function within the entity, whenever the entity materially changes its privacy policies or procedures.

(c) *Safeguards.*—(1) *Standard.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2) *Implementation specification: Verification procedures.* A covered entity must have administrative, technical, and physical procedures in place to protect the privacy of protected health information. Such procedures must include adequate procedures for verification of the identity and/or authority, as required by this subpart, of persons requesting such information, where such identity or authority is not known to the entity, as follows:

(i) The covered entity must use procedures that are reasonably likely to establish that the individual or person making the request has the appropriate identity for the use or disclosure requested, except for uses and disclosures that are:

(A) Permitted by this subpart and made on a routine basis to persons or other entities with which the covered entity interacts in the normal course of business or otherwise known to the covered entity; or

(B) Covered by paragraphs (c)(2)(ii), (iii), or (iv) of this section.

(ii) When the request for information is made by a government agency under § 164.510(b), § 164.510(c), § 164.510(e), § 164.510(f), § 164.510(g), § 164.510(m), § 164.510(n), or § 164.522, and the identity and/or authority are not known to the covered entity, the covered entity may not disclose such information without reasonable evidence of identity and/or authority to obtain the information.

(A) For purposes of this paragraph, "reasonable evidence of identity" means:

(*1*) A written request on the agency's letterhead;

(*2*) Presentation of an agency identification badge or official credentials; or

(*3*) Similar proof of government status.

(B) For purposes of this paragraph, *reasonable evidence of authority* means:

(*1*) A written statement of the legal authority under which the information is requested; a request for disclosure made by official legal process issued by a grand jury or a judicial or administrative body is presumed to constitute reasonable legal authority; or

(*2*) Where the request is made orally, an oral statement of such authority.

(iii) When the request for information is made by a person or entity acting on behalf of a government agency under § 164.510(b), § 164.510(c), § 164.510(g), or § 164.510(n), and the identity and/or authority are not known to the covered entity, the covered entity may not disclose such information without reasonable evidence of identity and/or authority to obtain the information.

(A) For the purposes of this paragraph, *reasonable evidence of identity* means:

(*1*) A written statement from the government agency, on the agency's letterhead, that the person or entity is acting under the agency's authority; or

(*2*) Other evidence or documentation, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person or entity is acting on behalf of or under the agency's authority.

(B) For the purposes of this paragraph, ''reasonable evidence of authority'' means a statement that complies with paragraph (c)(ii)(B) of this section.

(iv) For uses and disclosures under § 164.510(d), § 164.510(h), or § 164.510(j), compliance with the applicable requirements of those sections constitutes adequate verification under this section.

(v)(A) A covered entity may reasonably rely on evidence of identity and legal authority that meets the requirements of this paragraph.

(B) Where presentation of particular documentation or statements are required by this subpart as a condition of disclosure, a covered entity may reasonably rely on documentation or statements that on their face meet the applicable requirements.

(3) *Implementation specification: Other safeguards.* A covered entity must have safeguards to ensure that information is not used in violation of the requirements of this subpart or by members of its workforce or components of the entity or employees and other persons associated with, or components of, its business partners who are not authorized to access the information.

(4) *Implementation specification: Disclosures by whistleblowers.* A covered entity is not considered to have violated the requirements of this subpart where a member of its workforce or an employee or other person associated with a business partner discloses protected health information that such member or other person believes is evidence of a violation of law to:

(i) The law enforcement official or oversight agency authorized to enforce such law; or

(ii) An attorney, for the purpose of determining whether a violation of law has occurred or assessing what remedies or actions at law may be available to the employee.

(d) *Complaints to the covered entity*—(1) *Standard.* A covered entity that is a health plan or health care provider must provide a process whereby individuals may make complaints concerning the entity's compliance with the requirements established by this subpart.

(2) *Implementation specifications.* A covered entity that is a health plan or health care provider must develop and implement procedures under which an individual may file a complaint alleging that the covered entity failed to comply with one or more requirements of this subpart. Such procedures must provide for:

(i) The identification of the contact person or office required by paragraph (a)(2) of this section; and

(ii) Maintenance by the covered entity of a record of all complaints and their disposition, if any.

(e) *Sanctions: Standard.* A covered entity must develop and apply when appropriate sanctions against members of its workforce who fail to comply with the policies and procedures of the covered entity or the requirements of this subpart in connection with protected health information held by the covered entity or its business partners.

(f) *Duty to mitigate: standard.* A covered entity must have procedures for mitigating, to the extent practicable, any deleterious effect of a use or disclosure of protected health information in violation of this subpart.

§ 164.520 Documentation of policies and procedures.

(a) *Standard.* A covered entity must adequately document its compliance with the applicable requirements of this subpart.

(b) *Implementation specification: General.* A covered entity must document its policies and procedures for complying with the applicable requirements of this subpart. Such documentation must include, but is not limited to, documentation that meets the requirements of paragraphs (c) through (g) of this section.

(c) *Implementation specification: Uses and disclosures.* With respect to uses by the covered entity or its business partners of protected health information, a covered entity must document its policies and procedures regarding:

(1) Uses and disclosures of such information, including:

(i) Uses and disclosures with authorization, including for revocation of authorizations; and

(ii) Uses and disclosures without authorization, including:

(A) For treatment, payment, and health care operations;

(B) For disclosures to business partners, including monitoring and mitigation; and

(C) For uses and disclosures pursuant to § 164.510.

(2) For implementation of the minimum necessary requirement of § 164.506(b).

(3) For implementation of the right to request a restriction under § 164.506(c), including:

(A) Who, if anyone, in the covered entity is authorized to agree to such a request; and

(B) How restrictions agreed to are implemented.

(4) For creation of de-identified information in accordance with § 164.506(d).

(d) *Implementation specification: Individual rights.* A covered entity must document its policies and procedures under §§ 164.512, 164.514, 164.515, and 164.516, as applicable, including:

(1) How notices will be disseminated in accordance with § 164.512;

(2) Designated record sets to which access will be granted under § 164.514;

(3) Grounds for denying requests for access under § 164.514;

(4) Copying fees, if any;

(5) Procedures for providing accounting pursuant to § 164.515;

(6) Procedures for accepting or denying requests for amendment or correction under § 164.516;

(7) How other entities will be notified of amendments or corrections accepted under § 164.516; and

(8) Identification of persons responsible for making decisions or otherwise taking action, including serving as a contact person, under §§ 164.512, 164.514, 164.515, and 164.516.

(e) *Implementation specification: Administrative requirements.* A covered entity must provide documentation of its procedures for complying with § 164.518, including:

(1) Identification of the persons or offices required by § 164.518(a) and their duties;

(2) Training provided as required by § 164.518(b);

(3) How access to protected health information is regulated by the covered entity and its business partners, including safeguards required by § 164.518(c);

(4) For a covered entity that is a health plan or health care provider, for receiving complaints under § 164.518(d);

(5) Sanctions, and the application thereof, required by § 164.518(e); and

(6) Procedures for mitigation under § 164.518(f).

(f) *Implementation specification: Specific documentation required.* A covered entity must retain documentation of the following for six years from when the documentation is created, unless a longer period applies under this subpart:

(1) Restrictions agreed to pursuant to § 164.506(c);

(2) Contracts pursuant to § 164.506(e);

(3) Authorization forms used pursuant to § 164.508;

(4) Samples of all notices issued pursuant to § 164.512;

(5) Written statements required by § 164.514;

(6) The accounting required by § 164.515;

(7) Documents relating to denials of requests for amendment and correction pursuant to § 164.516;

(8) Certifications under § 164.518(b); and

(9) Complaints received and any responses thereto pursuant to § 164.518(d).

(g) *Implementation specification: Change in policy or procedure.* (1) Except as provided in paragraph (g)(2) of this section, a covered entity may not implement a change to a policy or procedure required or permitted under this subpart until it has made the appropriate changes to the documentation required by this section and the notice required by § 164.512.

(2) Where the covered entity determines that a compelling reason exists to make a use or disclosure or take another action permitted under this subpart that its notice and policies and procedures do not permit, it may make the use or disclosure or take the other action if:

(1) It documents the reasons supporting the use, disclosure, or other action; and

(2) Within 30 days of the use, disclosure, or other action, changes its notice, policies and procedures to permit such use, disclosure, or other action.

§ 164.522 Compliance and enforcement.

(a) *Principles for achieving compliance.*—(1) *Cooperation.* The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the requirements established under this subpart.

(2) *Assistance.* The Secretary may provide technical assistance to covered entities to help them comply voluntarily with this subpart.

(b) *Individual complaints to the Secretary.* An individual who believes that a covered entity is not complying with the requirements of this subpart may file a complaint with the Secretary, provided that, where the complaint relates to the alleged failure of a covered entity to amend or correct protected health information pursuant to § 164.516, the Secretary may determine whether the covered entity has followed procedures that comply with § 164.516, but will not determine whether the information involved is accurate, complete, or whether errors or omissions might have an adverse effect on the individual.

(1) *Requirements for filing complaints.* Complaints under this section must meet the following requirements:

(i) A complaint must be filed in writing, either on paper or electronically.

(ii) A complaint should name the entity that is the subject of the complaint and describe in detail the acts or omissions believed to be in violation of the requirements of this subpart.

(iii) The Secretary may prescribe additional requirements for the filing of complaints, as well as the place and manner of filing, by notice in the **Federal Register**.

(2) *Investigation.* The Secretary may investigate complaints filed under this section. Such investigation may include a review of the pertinent policies, practices, and procedures of the covered entity and of the circumstances regarding any alleged acts or omissions concerning compliance.

(c) *Compliance reviews.* The Secretary may conduct compliance reviews to determine whether covered entities are complying with this subpart.

(d) *Responsibilities of covered entities.*—(1) *Provide records and compliance reports.* A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the requirements of this subpart.

(2) *Cooperate with periodic compliance reviews.* The covered entity shall cooperate with the Secretary if the Secretary undertakes a review of the policies, procedures, and practices of a covered entity to determine whether it is complying with this subpart.

(3) *Permit access to information.* A covered entity must permit access by the Secretary during normal business hours to its books, records, accounts, and other sources of information, including protected health information, and its facilities, that are pertinent to ascertaining compliance with this subpart. Where any information required of a covered entity under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity must so certify and set forth what efforts it has made to obtain the information. Protected health information obtained in connection with a compliance review or investigation under this subpart will not be disclosed by the Secretary, except where necessary to enable the Secretary to ascertain compliance with this subpart, in formal enforcement proceedings, or where otherwise required by law.

(4) *Refrain from intimidating or retaliatory acts.* A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the filing of a complaint under this section, for testifying, assisting, participating in any manner in an investigation, compliance review, proceeding or hearing under this Act, or opposing any act or practice made unlawful by this subpart.

(e) *Secretarial action regarding complaints and compliance reviews.*—(1) *Resolution where noncompliance is indicated.* (i) If an investigation pursuant to paragraph (b)(2) of this section or a compliance review pursuant to paragraph (c) of this section indicates a failure to comply, the Secretary will so inform the covered entity and, where the matter arose from a complaint, the individual, and resolve the matter by informal means whenever possible.

(ii) If the Secretary determines that the matter cannot be resolved by informal means, the Secretary may issue written findings documenting the non-compliance to the covered entity and, where the matter arose from a complaint, to the complainant. The Secretary may use such findings as a basis for initiating action under section 1176 of the Act or initiating a criminal referral under section 1177.

(2) *Resolution where no violation is found.* If an investigation or compliance review does not warrant action pursuant

to paragraph (e)(1) of this section, the Secretary will so inform the covered entity and, where the matter arose from a complaint, the individual in writing.

§ 164.524 Effective date.

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

Appendix to Subpart E of Part 164—Model Authorization Form

AUTHORIZATION FOR RELEASE OF INFORMATION

Section A: Must be completed for all authorizations

I hereby authorize the use or disclosure of my individually identifiable health information as described below. I understand that this authorization is voluntary. I understand that if the organization authorized to receive the informatior is not a health plan or health care provider, the released information may no longer be protected by federal privacy regulations.

Patient name: ____________________ **ID Number:** ____________________

Persons/organizations providing the information: ____________________

Persons/organizations receiving the information: ____________________

Specific description of information (including date(s)): ____________________

Section B: Must be completed only if a health plan or a health care provider has requested the authorization

1. The health plan or health care provider must complete the following:
   a. What is the purpose of the use or disclosure?: ____________________
   b. Will the health plan or health care provider requesting the authorization receive financial or in-kind compensation in exchange for using or disclosing the health information described above? Yes______ No______

2. The patient or the patient's representative must read and initial the following statements:
   a. I understand that my health care and the payment for my health care will not be affected if I do not sign this form. Initials: ________
   b. I understand that I may see and copy the information described on this form if I ask for it, and that I get a copy of this form after I sign it. Initials: ________

Section C: Must be completed for all authorizations

The patient or the patient's representative must read and initial the following statements:
1. I understand that this authorization will expire on __ __/__ __/__ __ __ __ (DD/MM/YR) Initials: ________
2. I understand that I may revoke this authorization at any time by notifying the providing organization in writing, but if I do it won't have any affect on any actions they took before they received the revocation. Initials: ________

____________________ ____________________

Signature of patient or patient's representative **Date**
(Form MUST be completed before signing.)
Printed name of patient's representative: ____________________
Relationship to the patient: ____________________

**** YOU MAY REFUSE TO SIGN THIS AUTHORIZATION ****
You may not use this form to release information for treatment or payment except when the information to be released is psychotherapy notes or certain research information.

[FR Doc. 99–28440 Filed 10–28–99; 4:45 pm]
BILLING CODE 4150–04–C