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

[In dollars]

Provision	Initial or first year cost (2003, $million)	Average annual cost ($million, years 2–10)	Ten year cost (2003–2012) ($million)
Policy Development	597.7	0	597.7
Minimum Necessary	926.2	536.7	5,756.7
Privacy Officials	723.2	575.8	5,905.8
Disclosure Tracking/History	261.5	95.9	1,125.1
Business Associates	299.7	55.6	800.3
Notice Distribution	50.8	37.8	391.0
Consent	166.1	6.8	227.5
Inspection/Copying	1.3	1.7	16.8
Amendment	5.0	8.2	78.8
Requirements on Research	40.2	60.5	584.8
Training	287.1	50.0	737.2
De-Identification of Information	124.2	117.0	1,177.4
Employers with Insured Group Health Plans	52.4	0	52.4
Internal Complaints	6.6	10.7	103.2
Total*	3,242.0	1,556.9	17,554.7
Net Present Value	3,242.0	917.8	11,801.8

* **Note:** Numbers may not add due to rounding.

C. Need for the Final Rule

The need for a national health information privacy framework is described in detail in Section I of the preamble above. In short, privacy is a necessary foundation for delivery of high quality health care—the entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers. At the same time, there is increasing public concern about loss of privacy generally, and health privacy in particular. The growing use of interconnected electronic media for business and personal activities, our increasing ability to know an individual's genetic make-up, and the increasing complexity of the health care system each bring the potential for tremendous benefits to individuals and society, but each also brings new potential for invasions of our privacy.

Concerns about the lack of attention to information privacy in the health care industry are not merely theoretical. Section I of the preamble, above, lists numerous examples of the kinds of deliberate or accidental privacy violations that call for a national legal framework of health privacy protections. Disclosure of health information about an individual can have significant implications well beyond the physical health of that person, including the loss of a job, alienation of family and friends, the loss of health insurance, and public humiliation. The answer to these concerns is not for consumers to withdraw from the health care system, but for society to establish a clear national legal framework for privacy.

This section adds to the discussion in Section I, above, a discussion of the market failures inherent in the current system which create additional and compelling reasons to establish national health information privacy standards. 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 of health information concern information, negotiation, and enforcement costs between the entity and the individual. 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 protected health information will be used by that company. A health care provider or plan, for instance, knows many details about how protected health information may be generated, combined with other databases, or sold to third parties.

Absent this regulation, 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. A patient generally will have difficulty understanding medical records and the implications of transferring health information about them to a third party. Second, 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. These sorts of strategies, however, are both costly (in time and effort) and likely to be ineffective. 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. Therefore, the cost and ineffectiveness of monitoring leads to less than optimal protection of individually identifiable health information.

The incentives facing a company that acquires individually identifiable health information also discourage privacy protection. A company gains the full benefit of using such information, including its own marketing efforts or its ability to sell the information to third parties. The company, however, does not suffer the losses from disclosure of protected health information; the patient does. Because of imperfect monitoring, customers often will not

learn of, and thus not be able to take efficient action to prevent uses or disclosures of sensitive information. Because the company internalizes the gains from using the information, but does not bear a significant share, if any, of the cost to patients (in terms of lost privacy), it will have a systematic incentive to over-use individually identifiable health information. In market failure terms, companies will have an incentive to use individually identifiable health information where the patient would not have freely agreed to such use.

These difficulties are exacerbated 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 current system leads to significant market failures in bargaining privacy protection. Many privacy-protective agreements that patients would wish to make, absent barriers to bargaining, will not be reached.

The economic arguments become more compelling as the medical system shifts from predominantly paper to predominantly electronic records. Rapid changes in information technology should result in increased market failures in the markets for individually identifiable 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 health care providers and health 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 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 predominantly to electronic records in the near future, accompanying privacy rules will become more critical to prevent unanticipated, inappropriate, or unnecessary uses or disclosures of individually identifiable health information without 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 health plan is using health information about them. It will become more difficult to monitor the subsequent flows of individually identifiable 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 to 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 also 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, and HIV. Similarly, patients who are concerned about lack of privacy protections may report health information 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 forgone or inappropriate treatment.

In summarizing the economic arguments supporting the need for this regulation, the discussion here has emphasized the market failures that will be addressed by this regulation. These arguments become considerably stronger with the shift from predominantly paper to predominantly electronic records. 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, health 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.

D. Baseline Privacy Protections

An analysis of the costs and benefits of the regulation requires a baseline from which to measure the regulation's effects. For some regulations, the baseline is relatively straightforward. For instance, an industry might widely use a particular technology, but a new regulation may require a different technology, which would not otherwise have been adopted by the industry. In this example, the old and widely used technology provides the baseline for measuring the effects of the regulation. The costs and the benefits are the difference between keeping the old technology and implementing the new technology.

Where the underlying technology and industry practices are rapidly changing, however, it can be far more difficult to determine the baseline and thereby measure the costs and benefits of a regulation. There is no simple way to know what technology industry would have chosen to introduce if the regulation had never existed, nor how industry practices would have evolved.

Today, the entities covered by the HIPAA privacy regulation are in the midst of a shift from primarily paper records to electronic records. As covered entities spend significant resources on hardware, software, and other information technology costs, questions arise about which of these costs are fairly attributable to the privacy regulations as opposed to costs that would have been expended even in the absence of the regulations. Industry practices generally are rapidly evolving, as described in more detail in Part I of this preamble. New technological or other measure taken to protect privacy are in part attributable to the expected expense of shifting to electronic medical records, rather than being solely attributable to the new regulations. In addition, the existence of privacy rules in other sectors of the economy help set a norm for what practices will be considered good practices for health information. The level of privacy protection that would exist in the health care sector, in the absence of regulations, thus would likely be affected by regulatory and related developments in other sectors. In short, it is therefore difficult to project a cost or benefits baseline for this rule.

The common security practice of using ''firewalls'' illustrates how each of the three baselines might apply. Under the first baseline, the full cost of implementing firewalls should be included in a Regulatory Impact

Analysis for a rule that expects entities to have firewalls. Because current law has not required firewalls, a new rule expecting this security measure must include the full cost of creating firewalls. This approach, however, would seem to overstate the cost of such a regulation. Firewalls would seem to be an integral part of the decision to move to an on-line, electronic system of records. Firewalls are also being widely deployed by users and industries where no binding security or privacy regulations have been proposed.

Under the second baseline, the touchstone is the level of risk of security breaches for individually identifiable health information under current practices. There is quite possibly a greater risk of breach for an electronic system of records, especially where such records are accessible globally through the Internet, than for patient records dispersed among various doctors' offices in paper form. Using the second baseline, the costs of firewalls for electronic systems should not be counted as a cost of the regulation except where firewalls create greater security than existed under the previous, paper-based system.

Finally, the third baseline would require an estimate of the typical level of firewall protections that covered entities would adopt in the absence of regulation, and include in the Regulatory Impact Analysis only the costs that exceed what would otherwise have been adopted. For this analysis, the Department has generally assumed that the status quo would otherwise exist throughout the ten-year period (in a few areas we explicitly discuss likely changes). We made this decision for two reasons. First, predicting the level of change that would otherwise occur is highly problematic. Second, it is a ''conservative'' assumption—that is, any error will likely be an overstatement of the true costs of the regulation.

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 professional organizations and states have developed only limited guidelines for privacy practices, an entity may implement privacy practices independently. However, it is worth noting that changes in privacy protection continue to increase in various areas. For example, European Union countries may only send individually identifiable information to companies, including U.S. firms, that comply with their privacy standards, and the growing use of health data in other areas of commerce, such as finance and general commercial marketing, have also increased the demand for privacy in ways that were not of concern in the past.

1. Professional Codes of Ethics

The Department examined statements issued by five major professional groups, one national electronic network association and a leading managed care association.[38] 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;
- The development of policies to ensure the confidentiality of individually identifiable health information;
- A restriction that 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 individually identifiable health information. There is no common professional standard across the health care field with respect to the protection of individually identifiable health information. One critical area of difference is the extent to which professional organizations should release individually identifiable 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 its position by stating that the physician has the final word on whether a patient has access to his or her health information. This association also recommends that its members respond to requests for access to patient information within ten 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 his or her 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 individually identifiable health information.

The one set of standards that we reviewed from a health network association advocated the protection of individually identifiable health information from disclosure without patient authorization and emphasized that encrypting information should be a principal means of protecting individually identifiable health 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. The association suggested 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 rule as part of marketing activities.

Based on the review of the leading association standards, we believe that the final rule embodies most or all of the major principles expressed in the standards. However, there are some major areas of difference between the rule and the professional standards reviewed. The final rule generally provides stronger, more consistent, and more comprehensive guarantees of privacy for individually identifiable health information than the professional standards. The differences between the rule and the professional codes include the 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

[38] American Association of Health Plans, *Code of Conduct; http:www.aahp.org.;* American Dental Association, *Principles of Ethics and Professional Conduct; http://www.ada.org.*; American Hospital Association, ''Disclosure of Medical Record Information,'' *Management Advisory: Information Management*; 1990, AHA: Chicago, IL.; American Medical Association, *AMA Policy Finder—Current Opinions Council on Ethical and Judicial Affairs*; several documents available through the Policy Finder at *http:www.ama-assn.org.*; American Psychiatric Association, ''APA Outlines Standards Needed to Protect Patient's Medical Record''; Release No. 99–32, May 27, 1999; *http:www.psych.org.*

and the ability to respond to questions related to the notice. Because the regulation requires that (with a few exceptions) patients have access to their protected health information that a covered entity possesses, large numbers of health care 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 health care providers or health 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. The regulation allows for the release of protected health information for research purposes without an individual's authorization, but only if the research where such authorization is waived 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 complex, and often confusing, myriad of state laws and requirements. To determine whether or not the final rule would preempt a state law, first we identified the relevant laws, and second, we addressed whether state or federal law provides individuals with greater privacy protection.

Identifying the Relevant State Statutes: Health information privacy provisions can be found in laws applicable to many issues including insurance, worker's compensation, public health, birth and death records, adoptions, education, and welfare. 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. For example, Florida has over 60 laws that apply to protected health information. According to the Georgetown Privacy Project,[39] Florida is not unique. Every state has laws and regulations covering some aspect of medical information privacy. For the purpose of this analysis, we simply acknowledge the variation in state requirements.

We recognize that covered entities will need to learn the laws of their states in order to comply with such laws that are not contrary to the rule, or that are contrary to and more stringent than the rule. This analysis should be completed in the context of individual markets; therefore, we expect that professional associations or individual businesses will complete this task.

Recognizing the limits of our ability to effectively summarize state privacy laws, we discuss conclusions generated by the Georgetown University Privacy Project's report, *The State of Health Privacy: An Uneven Terrain.* The Georgetown report is among the most comprehensive examination of state health privacy laws currently published, although it is not exhaustive. The report, which was completed in July 1999, is based on a 50-state survey.

To facilitate discussion, we have organized the analysis into two sections: access to health information and disclosure of health information. Our analysis is intended to suggest areas where the final 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 some access to medical records about them. However, only a few states allow individuals access to health information held by all their health care providers and health plans. 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 about them held by health care 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 [40] 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 the purpose of the request and the facility holding the health information. 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. Many states allow fee structures, while eleven states specify only that the record holder may charge ''reasonable/actual costs.''

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.

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.[41]

Disclosure of Health Information: State laws vary widely with respect to disclosure of individually identifiable health information. Generally, states have applied restrictions on the disclosure of health information either to specific entities or for specific health conditions. Only three state laws place broad limits on disclosure of individually identifiable health information without regard for policies and procedures developed by covered entities. Most states require patient authorization before an entity may disclose health information to certain recipients, but the patient often does not have an opportunity to object to any disclosures.[42]

It is also important to point out that none of the states appear to offer individuals the right to restrict disclosure of their health information for treatment.

[39] Ibid, Goldman, p. 6.

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

[41] Ibid, Goldman, p. 20.

[42] Ibid, Goldman, p. 21.

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. Restrictions on re-disclosure of individually identifiable 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.

Most states have adopted specific measures to provide additional protections for health information regarding certain sensitive conditions or illnesses. The conditions and illnesses most commonly afforded added privacy protection are:

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

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 them an opportunity to object to the use of their information.[43]

Comparing state statutes to the final rule: The variability of state law regarding privacy of individually identifiable health information and the limitations of the applicability of many such laws demonstrates the need for uniformity and minimum standards for privacy protection. This regulation is designed to meet these goals while allowing stricter state laws to be enacted and remain effective. A comparison of state privacy laws with the final regulation highlights several of the 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 by this rule 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 rule will affect more entities than are covered or encompassed under many state laws.
- Among the three categories of covered entities, it appears that health plans will be the most significantly affected by the access provisions of the rule. Based on the Health Insurance Association of America (HIAA) data[44], there are approximately 94.7 million non-elderly persons with private health insurance in the 35 states that do not provide patients a legal right to inspect and copy their records.
- Under the rule, covered entities will have to obtain an 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. Although the final rule would establish a generally uniform disclosure and re-disclosure requirement for all covered entities, the entities that currently have the greatest ability and economic incentives to use and disclose protected health information for marketing services to both patients and health care providers without individual authorization.
- While the final 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 restrictions on disclosure, the rule will establish a baseline standard. But in states that do place conditions on the disclosure of protected health information, the rule may place additional requirements on covered entities.

3. Other Federal Laws

The relationship with other federal statutes is discussed above in the preamble.

E. Costs

Covered entities will be implementing the privacy final rules at the same time many of the administrative simplification standards are being implemented. As described in the overall impact analysis for the Transactions Rule, the data handling change occurring due to the other HIPAA standards will have both costs and benefits. To the extent the changes required for the privacy standards, implementation specifications, and requirements can be made concurrently with the changes required by the other regulations, costs for the combined implementation should be only marginally higher than for the administrative simplification standards alone. The extent of this incremental cost is uncertain, in the same way that the costs associated with each of the individual administrative simplification standards is uncertain.

The costs associated with implementing the requirements under this Privacy Rule will be directly related to the number of affected entities and the number of affected transactions in each entity. There are approximately 12,200 health plans (including self-insured employer and government health plans that are at least partially self-administered)[45], 6480 hospitals, and 630,000 non-hospital providers that will bear implementation costs under the final rule.

The relationship between the HIPAA security and privacy standards is particularly relevant. On August 17, 2000, the Secretary published a final rule to implement the HIPAA standards on electronic transactions. That rule adopted standards for eight electronic code sets to be used for those transactions. The proposed rule for security and electronic signature standards was published on August 12, 1998. That proposal specified the security requirements for covered entities that transmit and store information specified in Part C, Title II of the Act. In general, that proposed rule proposed administrative and technical standards for protecting ''* * * any health information pertaining to an individual that is electronically

[43] ''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.

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

[45] ''Health plans,'' for purposes of the regulatory impact and regulatory flexibility analyses, include licensed insurance carriers who sell health products; third party administrators that will have to comply with the regulation for the benefit of the plan sponsor; and self-insured health plans that are at least partially administered by the plan sponsor.

maintained or transmitted.'' (63 FR 43243). The final Security Rule will detail the system and administrative requirements that a covered entity must meet in order to assure itself and the Secretary that health information is safe from destruction and tampering from people without authorization for its access.

By contrast, the Privacy Rule describes the requirements that govern the circumstances under which protected health information must be used or disclosed with and without patient involvement and when a patient may have access to his or her protected health information.

While the vast majority of health care entities are privately owned and operated, we note that federal, state, and local government providers are reflected in the total costs as well. Federal, state, and locally funded hospitals represent approximately 26 percent of hospitals in the United States. This is a significant portion of hospitals, but it represents a relatively small proportion of all provider entities. We estimated that the number of government providers who are employed at locations other than government hospitals is significantly smaller (approximately two 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. Indian Health Service 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 developing the 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.

The costs associated with this final rule involve, for each provision, consideration of both the degree to which covered entities must modify their existing records management systems and privacy policies under the final rule, and the extent to which there is a change in behavior by both patients and the covered entities as a result of the final rule. The following sections examine these provisions as they apply to the various covered entities under the final rule. The major costs that covered entities will incur are one-time costs associated with implementation of the final rules, and ongoing costs that result in continuous requirements in the final rule.

The Department has quantified the costs imposed by the final regulation to the extent possible. The cost of many provisions were estimated by first using data from the Census Bureau's Statistics of U.S. Business to identify the number of non-hospital health care providers, hospitals and health plans. Then, using the Census Bureau's Current Population Survey (CPS) wage data for the classes of employees affected by the rule, the Department identified the hourly wage of the type of employee assumed to be mostly likely responsible for compliance with a given provision. Where the Department believed a number of different types of employees might be responsible for complying with a certain provision, as is often expected to be the case, the Department established a weighted-average wage based on the types of employees involved. Finally, the Department made assumptions regarding the number of person-hours per institution required to comply with the rule.

The Department cannot determine precisely how many person-hours per institution will be required to comply with a given provision, however, the Department attempted to establish reasonable estimates based on fact-finding discussions with private sector health care providers, the advice of the Department's consultants, and the Department's own best judgement of the level of burden required to comply with a given provision. Moreover, the Department recognizes that the number of hours required to comply with a given requirement of the rule will vary from provider to provider and health plan to health plan, particularly given the flexibility and scalability permitted under the rule. Therefore, the Department considers the estimates to be averages across the entire class of health care providers, hospitals, or health plans in question.

Underlying all annual cost estimates are growth projections. For growth in the number of patients, the Department used data from the National Ambulatory Medical Care Survey, the National Hospital Ambulatory Medical Care Survey, the National Home and Hospice Survey, the National Nursing Home Survey, and information from the American Hospital Association. For growth in the number of health care workers, the Department used data from the Bureau of Health Professions in the Department's Health Resources Services Administration (HRSA). For insurance coverage growth (private and military coverage), we used a five-year average annual growth rate in employer-sponsored, individual, military, and overall coverage growth from the Census Bureau's CPS, 1995–1999. To estimate growth in the number of Medicare and Medicaid enrollees, the Department used the enrollment projections of the Health Care Financing Administration's Office of the Actuary. For growth in the number of hospitals, health care providers and health plans, trend rates were derived from the Census Bureau's Statistics of U.S. Businesses, using SIC code-specific five-year annual average growth rate from 1992–1997 (the most recent data available). For wage growth, the Department used the same assumptions made in the Medicare Trustees' Hospital Insurance Trust Fund report for 2000.

In some areas, the Department was able to obtain very reliable data, such as survey data from the Statistics of U.S. Businesses and the Medical Expenditures Panel Survey (MEPS). In numerous areas, however, there was too little information or data to support quantitative estimates. As a result, the Department relied on data provided in the public comments or subsequent fact-finding to provide a basis for making key assumptions. We were able to provide a reasonable cost estimate for virtually all aspects of the regulation, except law enforcement. In this latter area, the Department was unable to obtain sufficient data about current practices (*e.g.,* the number of criminal and civil investigations that may involve requests for protected health information, the number of subpoenas for protected health information, etc.) to determine the marginal effects of the regulation. As discussed more fully below, the Department believes the effects of the final rule are marginal because the policies adopted in the final rule appear to largely reflect current practice.

The NPRM included an estimate of $3.8 billion for the privacy proposal. The estimate for the final rule is $18.0 billion. Much of the difference can be explained by two factors. First, the NPRM estimate was for five years; the final rule estimate is for ten years. The Department chose the longer period for the final rule because ten years was also the period of analysis in the Transactions Rule RIA, and we wanted to facilitate comparisons, given that the net benefits and costs of the administrative simplification rules should be considered together. Second, the final impact analysis includes cost estimates for a number of key provisions that were not estimated in the NPRM because the Department did not have adequate information at the time.

Although we received little useable data in the public comments (see comment and response section), the Department was able to undertake more extensive fact-finding and collect sufficient information to make informed assumptions about the level of effort and time various provisions of the final rule are likely to impose on different types of affected entities.

The estimate of $18.0 billion represents a gross cost, not a net cost. As discussed more fully below in the benefits section, the benefits of enhanced privacy and confidentiality of personal health information are very significant. If people believe their information will be used properly and not disseminated beyond certain bounds without their knowledge and consent, they will be much more likely to seek proper health care, provide all relevant health information, and abide by their providers' recommendations. In addition, more confidence by individuals and covered entities that privacy will be maintained will lead to an increase in electronic transactions and the efficiencies and cost savings that stem from such action. The benefits section quantifies some examples of benefits. The Department was not able to identify data sources or models that would permit us to measure benefits more broadly or accurately. The inability to quantify benefits, however, does not lessen the importance or value that is ultimately realized by having a national standard for health information privacy.

The largest initial costs resulting from the final Privacy Rule stem primarily from the requirement that covered entities use and disclose only the minimum necessary protected health information, that covered entities develop policies and codify their privacy procedures, and that covered entities designate a privacy official and train all personnel with access to individually identifiable health information. The largest ongoing costs will result from the minimum necessary provisions pertaining internal uses of individually identifiable health information, and the cost of a privacy official. In addition, covered entities will have recurring costs for training, disclosure tracking and notice requirements. A smaller number of large entities may have significant costs for de-identification of protected health information and additional requirements for research.

The privacy costs are in addition to the Transactions Rule estimates. The cost of complying with the regulation represents approximately 0.23 percent of projected national health expenditures the first year the regulation is enacted. The costs for the first eight years of the final regulation represents 0.07 percent of the increase in national health care costs experienced over the same period.[46]

Minimum Necessary

The ''minimum necessary'' policy in the final rule has essentially three components: first, it does not pertain to certain uses and disclosures including treatment-related exchange of information among health care providers; second, for disclosures that are made on a routine and recurring basis, such as insurance claims, a covered entity is required to have policies and procedures for governing such exchanges (but the rule does not require a case-by-case determination); and third, providers must have a process for reviewing non-routine requests on a case-by-case basis to assure that only the minimum necessary information is disclosed.

Based on public comments and subsequent fact-finding, the Department has concluded that the requirements of the final rule are generally similar to the current practice of most providers. For standard disclosure requests, for example, providers generally have established procedures for determining how much health information is released. For non-routine disclosures, providers have indicated that they currently ask questions to discern how much health information is necessary for such disclosure. Under the final rule, we anticipate providers will have to be more thorough in their policies and procedures and more vigilant in their oversight of them; hence, the costs of this provision are significant.

To make the final estimates for this provision, the Department considered the minimum necessary requirement in two parts. First, providers, hospitals, and health plans will need to establish policies and procedures which govern uses and disclosures of protected health information. Next, these entities will need to adjust current practices that do not comply with the rule, such as updating passwords and making revisions to software.

To determine the policies and procedures for the minimum necessary requirement, the Department assumed that each hospital would spend 160 hours, health plans would spend 107 hours, and non-hospital providers would spend 8 hours. As noted above, the time estimates for this and other provisions of the rule are considered an average number of person-hours for the institutions involved. An underlying assumption is that some hospitals, and to a lesser extent health plans, are part of chains or larger entities that will be able to prepare the basic materials at a corporate level for a number of covered entities.

Once the policies and procedures are established, the Department estimates there will be costs resulting from implementing the new policies and procedures to restrict internal uses of protected health information to the minimum necessary. Initially, this will require 560 hours for hospitals, 160 hours for health plans, and 12 hours for non-hospital providers.[47] The wage for health care providers and hospitals is estimated at $47.28, a weighted average of various health care professionals based on CPS data; the wage for health plans is estimated to be $33.82, based on average wages in the insurance industry (note that all wage assumptions in this impact analysis assume a 39 percent load for benefits, the standard Bureau of Labor Statistics assumption). In addition, there will be time required on an annual basis to ensure that the implemented practices continue to meet the requirements of the rule. Therefore, the Department estimates that on an annual ongoing basis (after the first year), hospitals will require 320 hours, health plans 100 hours, and non-hospital providers 8 hours to comply with this provision.

The initial cost attributable to the minimum necessary provision is $926 million. The total cost of the provision is $5.757 billion. (These estimates are for the cost of complying with the minimum necessary provisions that restrict internal uses to the minimum necessary. The Department has estimated in the business associates section below the requirement limiting disclosures outside the covered entity to the minimum amount necessary.)

Privacy Official

The final rule requires entities to designate a privacy official who will be responsible for the development and implementation of privacy policies and procedures. In this cost analysis, the Department has estimated each of the primary administrative requirements of the rule (e.g., training, policy and

[46] Health Care Finance Administration, Office of the Actuary, 2000. Estimates for the national health care expenditure accounts are only available through 2008; hence, we are only able to make the comparison through that year.

[47] These estimates were, in part, derived from a report prepared for the Department by the Gartner Group, consultants in health care information technology: ''Gartner DHHS Privacy Regulation Study,'' by Jim Klein and Wes Rishel, submitted to the Office of the Assistant Secretary for Policy and Evaluation on October 20, 2000.

procedure development, etc), including the development and implementation costs associated with each specific requirement. These activities will certainly involve the privacy official to some degree; thus, some costs for the privacy official, particularly in the initial years, are subsumed in other cost requirements. Nonetheless, we anticipate that there will be additional ongoing responsibilities that the privacy official will have to address, such as coordinating between departments, evaluating procedures and assuring compliance. To avoid double-counting, the cost calculated in this section is only for the ongoing, operational functions of a privacy official (e.g., clarifying procedures for staff) that are in addition to items discussed in other sections of this impact analysis.

The Department assumes the privacy official role will be an additional responsibility given to an existing employee in the covered entity, such as an office manager in a small entity or a compliance official in a larger institution. Moreover, today any covered entity that handles individually identifiable health information has one or more people with responsibility for handling and protecting the confidentiality of such information. As a result of the specific requirement for a privacy official, the Department assumes covered entities will centralize this function, but the overall effort is not likely to increase significantly. Specifically, the Department has assumed non-hospital providers will need to devote, on average, an additional 30 minutes per week of an official's time (i.e., 26 hours per year) to compliance with the final regulation for the first two years and 15 minutes per week for the remaining eight years (i.e., 13 hours per year). For hospitals and health plans, which are more likely to have a greater diversity of activities involving privacy issues, we have assumed three hours per week for the first two years (i.e., 156 hours per year), and 1.5 hours per week for the remaining eight years (i.e., 78 hours per year).

For non-hospital providers, the time was calculated at a wage of $34.13 per hour, which is the average wage for managers of medicine and health according to the CPS. For hospitals, we used a wage of $79.44, which is the rate for senior planning officers.[48] For health plans, the Department assumed a wage of $88.42 based on the wage for top claims executives.[49] Although individual hospitals and health plans may not necessarily select their planning officers or claims executives to be their privacy officials, we believe they will be of comparable responsibility, and therefore comparable pay, in larger institutions.

The initial year cost for privacy officials will be $723 million; the ten-year cost will be $5.9 billion.

Internal Complaints

The final rule requires each covered entity to have an internal process to allow an individual to file a complaint concerning the covered entity's compliance with its privacy policies and procedures. The requirement includes designating a contact person or office responsible for receiving complaints and documenting the disposition of them, if any. This function may be performed by the privacy official, but because it is a distinct right under the final rule and may be performed by someone else, we are costing it separately.

The covered entity only is required to receive and document a complaint (no response is required), which we assume will take, on average, ten minutes (the complaint can be oral or in writing). The Department believes that such complaints will be uncommon. We have assumed that one in every thousand patients will file a complaint, which is approximately 10.6 million complaints over ten years. Based on a weighted-average hourly wage of $47.28 at ten minutes per complaint, the cost of this policy is $6.6 million in the first year. Using wage growth and patient growth assumptions, the cost of this policy is $103 million over ten years.

Disclosure Tracking and History

The final rule requires providers to be able to produce a record of all disclosures of protected health information, except in certain circumstances. The exceptions include disclosures for treatment, payment, health care operations, or disclosures to an individual. This requirement will require a notation in the record (electronic or paper) of when, to whom, and what information was disclosed, as well as the purpose of such disclosure or a copy of an individual's written authorization or request for a disclosure.

Based on information from several hospital sources, the Department assumes that all hospitals already track disclosures of individually identifiable health information and that 15 percent of all patient records held by a hospital will have an annual disclosure that will have to be recorded in an individual's record. It was more difficult to obtain a reliable estimate for non-hospital providers, though it appears that they receive many fewer requests. The Department assumed a ten percent rate for ambulatory care patients and five percent, for nursing homes, home health, dental and pharmacy providers. (It was difficult to obtain any reliable data for these latter groups, but those we talked to said that they had very few, and some indicated that they currently keep track of them in the records.) These estimated percentages represent about 63 million disclosures that will have to be recorded in the first year, with each recording estimated to require two minutes. At the average nurse's salary of $30.39 per hour, the cost in the first year is $25.7 million. For health plans, the Department assumed that disclosures of protected health information are more rare than for health care providers. Therefore, the Department assumed that there will be disclosures of protected health information for five percent of covered lives. At the average wage for the insurance industry of $33.82 per hour, the initial cost for health plans is $6.8 million. Using our standard growth rates for wages, patients, and covered entities, the ten-year cost for providers and health plans is $519 million.

In addition, although hospitals generally track patient disclosures today, the Department assumes that hospitals will seek to update software systems to assure full compliance. Based on software upgrade costs provided by the Department's private sector consultants with expertise in the area (the Gartner Group), the Department assumed that each upgrade would cost $35,000 initially and $6,300 annually thereafter, for a total cost of $572 million over ten years.

The final rule also requires covered entities to provide individuals with an accounting of disclosures upon request. The Department assumes that few patients will request a history of disclosures of their protected medical information. Therefore, we estimate that one in a thousand patients will request such an accounting each year, which is approximately 850,000 requests. If it takes an average of five minutes to copy any disclosures and the work is done by a nurse, the cost for the first year will be $2.1 million. The total ten-year cost is $33.8 million.

[48] ''Top Compensation in the Healthcare Industry, 1997'', Coopers & Lybrand, New York, NY., <http://www.pohly.com/salary/2.shtml>.

[49] ''A Unifif Survey of Compensation in Financial Services: 2000,'' July 2000, Unifi Network Survey unit, PriceWaterhouseCoopers LLP and Global HR Solutions LLC, Westport, Ct., <http://public.wsj.com/careers/resources/documents/20000912-insuranceexecs-tab.htm>.

De-Identification of Information

The rule allows covered entities to determine that health information is de-identified (i.e., that it is not individually identifiable health information) if certain conditions are met. Currently, some entities release de-identified information for research purposes. De-identified information may originate from automated systems (such as records maintained by pharmacy benefit managers) and non-automated systems (such as individual medical records maintained by providers). As compared with current practice, the rule requires that an expanded list of identifiers be removed for the data (such as driver's license numbers, and detailed geographic and certain age information). For example, as noted in a number of public comments, currently complete birth dates (day, month, and year) and zip codes are often included in de-identified information. The final rule requires that only the year of birth (except in certain circumstances) and the first three digits of the zip code can be included in de-identified information.

These changes will not require extensive change from current practice. Providers generally remove most of the 19 identifiers listed in the final rule. The Department relied on Gartner Group estimates that some additional programmer time will be required by covered entities that produce de-identified information to make revisions in their procedures to eliminate additional identifiers. Entities that de-identify information will have to review existing and future data flows to assure compliance with the final rule. For example, an automated system may need to be re-programmed to remove additional identifiers from otherwise protected health information. (The costs of educating staff about the de-identification requirements are included in the cost estimate for training staff on privacy policies.)

The Department was not able to obtain any reliable information on the volume of medical data that is currently de-identified. To provide some measure of the potential magnitude, we assumed that health plans and hospitals would have an average of two existing agreements that would need to be reviewed and modified. Based on information provided by our consultants, we estimate that these agreements would require an average of 152 hours by hospitals and 116 hours by health plans to review and revise existing agreements to conform to the final rule. Using the weighted average wage of $47.28, the initial costs will be $124 million. Using our standard growth rates for wages, patients, and covered entities, the total cost of the provision is $1.1 billion over ten years.

The Department expects that the final rule and the increasing trend toward computerization of large record sets will result over time in de-identification being performed by relatively few firms or associations. Whether the covered entity is a small provider with relatively few files or a hospital or health plan with large record files, it will be more efficient to contract with specialists in these firms or associations (as ''business associates'' of the covered entity) to de-identify files. The process will be different but the ultimate cost is likely to be the same or only slightly higher, if at all, than the costs for de-identification today. The estimate is for the costs required to conform existing and future agreements to the provisions of the rule. The Department has not quantified the benefits that might arise from changes in the market for de-identified information because the centralization and efficiency that will come from it will not be fully realized for several years, and we do not have a reliable means of estimating such changes.

Policy and Procedures Development

The final regulation imposes a variety of requirements which collectively will necessitate entities to develop policies and procedures (henceforth in this section to be referred to as policies) to establish and maintain compliance with the regulation. These include policies such as those for inspection and copying, amending records, and receiving complaints.[50] In developing the final regulations, simplifying the administrative burden was a significant consideration. To the extent practical, consistent with maintaining adequate protection of protected health information, the final rule is designed to encourage the development of policies by professional associations and others, that will reduce costs and facilitate greater consistency across providers and other covered entities.

The development of policies will occur at two levels: first, at the association or other large scale levels; and second, at the entity level. Because of the generic nature of many of the final rule's provisions, the Department anticipates that trade, professional associations, and other groups serving large numbers of members or clients will develop materials that can be used broadly. These will likely include the model privacy practice notice that all covered entities will have to provide patients; general descriptions of the regulation's requirements appropriate for various types of health care providers; checklists of steps entities will have to take to comply; training materials; and recommended procedures or guidelines. The Department spoke with a number of professional associations, and they confirmed that they would expect to provide such materials for their members at either the federal or state level.

Using Faulkner and Gray's *Health Data Directory 2000*, we identified 216 associations that would be likely to provide guidance to members. In addition, we assume three organizations (i.e., one for hospitals, health plans, and other health care providers) in each state would also provide some additional services to help covered entities coordinate the requirements of this rule with state laws and requirements. The Department assumed that these associations would each provide 320 hours of legal analysis at $150 per hour, and 640 hours of senior analysts time at $50 per hour. This equals $17.3 million. Hourly rates for legal council are the average billing rate for a staff attorney.[51] The senior analysts rates are based on a salary of $75,000 per year, plus benefits, which was provided by a major professional association.

For larger health care entities such as hospitals and health plans, the Department assumed that the complexity of their operations would require them to seek more customized assistance from outside council or consultants. Therefore, the Department assumes that each hospital and health plan (including self-administered, self-insured health plans) will, on average, require 40 hours of outside assistance. The resulting cost for external policy development is estimated to be $112 million.

All covered entities are expected to require some time for internal policy development beyond what is provided by associations or outside consultants. For most non-hospital providers, the external assistance will provide most of the necessary information. Therefore, we expect these health care providers will need only eight hours to adapt these policies for their specific use (training cost is estimated separately in the impact analysis). Hospitals and

[50] The cost for policies for minimum necessary, because they will be distinct and extensive, are presented separately, above.

[51] ''The Altman Weil 1999 Survey of Law Firm Economics,'' <*http://www.altmanweil.com/publications/survey/sife99/standard.htm*>.

health plans, which employ more individuals and are involved in a wider array of endeavors, are likely to require more specific policies tailored to their operations to comply with the final rule. For these entities, we assume an average of 320 hours of policy development per institution. The total cost for internal policy development is estimated to be $468 million.

The total cost for policy, plan, and procedures development for the final regulation is estimated to be $598 million. All of these costs are initial costs.

Training

The final regulation's requirements provide covered entities with considerable flexibility in how to best fulfill the necessary training of their workforce. As a result, the actual practices may vary substantially based on such factors as the number of members of the workforce, the types of operations, worker turnover, and experience of the workforce. Training is estimated to cost $737 million over ten years. The Department estimates that at the time of the effective date, approximately 6.7 million health care workers will have to be trained, and in the subsequent ten years, 7 million more will have to be trained because of worker turnover. The estimate of employee numbers are based on 2000 CPS data regarding the number of health care workers who indicated they worked for a health care institution. To estimate a workforce turnover rate, the Department relied on a study submitted in the public comments which used a turnover rate of ten percent or less, depending on the labor category. To be conservative, the Department assumed ten percent for all categories.

Covered entities will need to provide members of the workforce with varying amounts of training depending on their responsibilities, but on average, the Department estimates that each member of the workforce who is likely to have access to protected health information will require one hour of training in the policies and procedures of the covered entity. The initial training cost estimate is based on teacher training with an average class size of ten. After the initial training, the Department expects some training (for example, new employees in larger institutions) will be done by videotape, video conference, or computer, all of which are likely to be less expensive. Training materials were assumed to cost an average of $2 per worker. The opportunity cost for the training time is based on the average wage for each health care labor category listed in the CPS, plus a 39 percent load for benefits. Wages were increased based on the wage inflation factor utilized for the short-term assumptions (which covers ten years) in the Medicare Trustees' Annual Report for 1999.

Notice

This section describes only the cost associated with the production and provision of a notice. The cost of developing the policy stated in the notice is covered under policies and procedures, above.

Covered health care providers with direct treatment relationships are required to provide a notice of privacy practices no later than the date of the first service delivery to individuals after the compliance date for the covered health care provider. The Department assumed that for most types of health care providers (such as physicians, dentists, and pharmacists) one notice would be distributed to each patient during his or her first visit following the compliance date for the covered provider, but not for subsequent visits. For hospitals, however, the Department assumed that a notice would be provided at each admission, regardless of how many visits an individual has in a given year. In subsequent years, the Department assumed that non-hospital providers would only provide notices to their new patients, because it is assumed that providers can distinguish between new and old patients, although hospitals will continue to provide a notice for each admission. The total number of notices provided in the initial year is estimated to be 816 million.

Under the final rule, only providers that have direct treatment relationships with individuals are required to provide notices to them. To estimate the number of visits that trigger a notice in the initial year and in subsequent years, the Department relied on the Medical Expenditure Panel Survey (MEPS, 1996 data) conducted by the Department's Agency for Healthcare Quality and Research. This data set provides estimates for the number of total visits to a variety of health care providers in a given year and estimates of the number of patients with at least one visit to each type of each care provider. To estimate the number of new patients in a given year, the Department used the National Ambulatory Medical Care Survey and the National Hospital Ambulatory Medical Care Survey, which indicate that for ambulatory care visits to physician offices and hospital ambulatory care departments, 13 percent of all patients are new. This data was used as a proxy for other types of providers, such as dentists and nursing homes, because the Department did not have estimates for new patients for other types of providers. The number of new patients was increased over time to account for growth in the patient population. Therefore, the number of notices provided in years 2004 through 2012 is estimated to be 5.3 billion.

For health plans, the Department estimated the number of notices by trending forward the average annual rate of growth from 1995 through 1998 (the most recent data available) of private policy holders using the Census Bureau's Current Population Survey, and also by using Health Care Financing Administration Office of the Actuary's estimates for growth in Medicare and Medicaid enrollment. It should be noted that the regulation does not require that the notice be mailed to individuals. Therefore, the Department assumed that health plans would include their privacy policy in the annual mailings they make to members, such as by adding a page to an existing information booklet.

Since clinical laboratories generally do not have direct contact with patients, they would not normally be required to provide notices. However, there are some laboratory services that involve direct patient contact, such as patients who have tests performed in a laboratory or at a health fair. We found no data from which we could estimate the number of such visits. Therefore, we have assumed that labs would incur no costs as a result of this requirement.

The printing cost of the policy is estimated to be $0.05, based on data obtained from the Social Security Administration, which does a significant number of printings for distribution. Some large bulk users, such as health plans, can probably reproduce the document for less, and small providers simply may copy the notice, which would also be less than $0.05. Nonetheless, at $0.05, the total cost of the initial notice is $50.8 million.

Using our standard growth rate for patients, the total cost for notices is estimated to be $391 million for the ten-year period.

Requirements on Use and Disclosure for Research

The final regulation places certain requirements on covered entities that supply individually identifiable health information to researchers. As a result of these requirements, researchers who seek such health information and the Institutional Review Boards (IRBs) that review research projects will have additional responsibilities. Moreover, a covered entity doing research, or another entity requesting disclosure of

protected health information for research that is not currently subject to IRB review (research that is 100 percent privately funded and which takes place in institutions which do not have ''multiple project assurances'') may need to seek IRB or privacy board approval if they want to avoid the requirement to obtain authorization for use or disclosure of protected health information for research, thereby creating the need for additional IRBs and privacy boards that do not currently exist.

To estimate the additional requirements placed on existing IRBs, the Department relied on a survey of IRBs conducted by James Bell Associates on behalf of NIH and on estimates of the total number of existing IRBs provided by NIH staff. Based on this information, the Department concluded that of the estimated 4,000 IRBs in existence, the median number of initial current research project reviews is 133 per IRB, of which only ten percent do not receive direct consent for the use of protected health information. (Obtaining consent nullifies the need for IRB privacy scrutiny.) Therefore, in the first year of implementation, there will be 76,609 initial reviews affected by the regulation, and the Department assumes that the requirement to consider the privacy protections in the research protocols under review will add an average of 1 hour to each review. The cost to researchers for having to develop protocols which protect protected health information is difficult to estimate, but the Department assumes that each of the affected 76,609 studies will require an average of an additional 8 hours of time for protocol development and implementation. At the average medical scientist hourly wage of $46.61, the initial cost is $32.1 million; the total ten-year cost of these requirements is $468 million over ten years.

As stated above, some privately funded research not subject to any IRB review currently may need to obtain IRB or privacy board approval under the final rule. Estimating how much research exists which does not currently go through any IRB review is highly speculative, because the experts consulted by the Department all agree that there is no data on the volume of privately funded research. Likewise, public comments on this subject provided no useful data. However, the Department assumed that most research that takes place today is subject to IRB review, given that so much research has some government funding and many large research institutions have multiple project assurances. As a result, the Department assumed that the total volume of non-IRB reviewed research is equal to 25 percent of all IRB-reviewed research, leading to 19,152 new IRB or privacy board reviews in the first year of the regulation. Using the same assumptions as used above for wages, time spent developing privacy protection protocols for researchers, and time spent by IRB and privacy board members, the total one-year cost for new IRB and privacy board reviews is $8 million.

For estimating total ten-year costs, the Department used the Bell study, which showed an average annual growth rate of 3.7 percent in the number of studies reviewed by IRBs. Using this growth rate, the total ten-year cost for the new research requirements is $117 million.

Consent

Under the final rule, a covered health care provider with direct treatment relationships must obtain an individual's consent for use or disclosure of protected health information for treatment, payment, or health care operations. Covered providers with indirect treatment relationships and health plans may obtain such consent if they so choose. Providers and health plans that seek consent under this rule can condition treatment or enrollment upon provision of such consent. Based on public comments and discussions with a wide array of health care providers, it is apparent that most currently obtain written consent for use and disclosure of individually identifiable health information for payment. Under the final rule, they will have to obtain consent for treatment and health care operations, as well, but this may entail only minor changes in the language of the consent to incorporate these other categories and to conform to the rule.

Although the Department was unable to obtain any systematic data, the anecdotal evidence suggests that most non-hospital providers and virtually all hospitals follow this practice. For the cost analysis, the Department assumes that 90 percent of the non-hospital providers and all hospitals currently obtain some consent for use and disclosure of individually identifiable health information. For providers that currently obtain written consent, there is only a nominal cost for changing the language on the document to conform to the rule. For this activity, we assumed $0.05 cost per document for revising existing consent documents.

For the ten percent of treating providers who currently do not obtain consent, there is the cost of creating consent documents (which will be standardized), which is also assumed to be $0.05 per document. It is assumed that all providers required to obtain consent under the rule will do so upon the first visit, so there will be no mailing cost. For non-hospital providers, we assume the consent will be maintained in paper form, which is what most providers currently do (electronic form, if available, is cheaper to maintain). There is no new cost for records maintenance because the consent will be kept in active files (paper or electronic).

The initial cost of the consent requirement is estimated to be $166 million. Using our standard assumptions for patient growth, the total costs for the ten years is estimated to be $227 million.

Authorizations

Patient authorizations are required for uses or disclosures of protected health information that are not otherwise explicitly permitted under the final rule with or without consent. In addition to uses and disclosures of protected health information for treatment, payment, and health care operations with or without consent, the rule also permits certain uses of protected health information, such as fund-raising for the covered entity and certain types of marketing activity, without prior consent or authorization. Authorizations are generally required if a covered entity wants to provide protected health information to third party for use by the third party for marketing or for research that is not approved by an IRB or privacy board.

The requirement for obtaining authorizations for use or disclosure of protected health information for most marketing activity will make direct third-party marketing more difficult because covered entities may not want to obtain and track such authorizations, or they may obtain too few to make the effort economically worthwhile. However, the final rule permits an alternative arrangement: the covered entity can engage in health-related marketing on behalf of a third party, presumably for a fee. Moreover, the covered entity could retain another party, through a business associate relationship, to conduct the actual health-related marketing, such as mailings or telemarketing, under the covered entity's name. The Department is unable to estimate the cost of these changes because there is no credible data on the extent of current third party marketing practices or the price that third party marketers currently pay for information from covered entities. The effect of the final rule is to change the

arrangement of practices to enhance accountability of protected health information by the covered entity and its business associates; however, there is nothing inherently costly in these changes.

Examples of other circumstances in which authorizations are required under the final rule include disclosure of protected health information to an employer for an employment physical, pre-enrollment underwriting for insurance, or the sharing of protected health insurance information by an insurer with an employer. The Department assumes there is no new cost associated with these requirements because providers have said that obtaining authorization under such circumstances is current practice.

To use or disclose psychotherapy notes for most purposes (including for treatment, payment, or health care operations), a covered entity must obtain specific authorization by the individual that is distinct from any authorization for use and disclosure of other protected health information. This is current practice, so there is no new cost associated with this provision.

Confidential Communications

The final rule permits individuals to receive communications of protected health information from a covered health care provider or a health plan by an alternative means or at an alternative address. A covered provider and a health plan must accommodate reasonable requests; however, a health plan may require the individual to state that disclosure of such information may endanger the individual. A number of providers and health plans indicated that they currently provide this service for patients who request it. For providers and health plans with electronic records system, maintaining separate addresses for certain information is simple and inexpensive, requiring little or no change in the system. For providers with paper records, the cost may be higher because they will have to manually check records to determine which information must be treated in accordance with such requests. Although some providers currently provide this service, the Department was unable to obtain any reliable estimate of the number of such requests today or the number of providers who perform this service. The cost attributable to this requirement to send materials to alternate addresses does not appear to be significant.

Employers With Insured Group Health Plans

Some group health plans will use or maintain protected health information, particularly group health plans that are self-insured. Also, some plan sponsors that perform administrative functions on behalf of their group health plans, may need protected health information. The final rule permits a group health plan, or a health insurance issuer or HMO that provides benefits on behalf of the group health plan, to disclose protected health information to a plan sponsor who performs administrative functions on its behalf for certain purposes and if certain requirements are met. The plan documents must be amended to: describe the permitted uses and disclosures of protected health information by the plan sponsor; specify that disclosure is permitted only upon receipt of a certification by the plan sponsor that the plan documents have been amended and the plan sponsor agrees to certain restrictions on the use of protected health information; and provide for adequate firewalls to assure unauthorized personnel do not have access to individually identifiable health information.

Some plan sponsors may need information, not to administer the group health plan, but to amend, modify, or terminate the plan. ERISA case law describes such activities as settlor functions. For example, a plan sponsor may want to change its contract from a preferred provider organization to a health maintenance organization (HMO). In order to obtain premium information, the plan sponsor may need to provide the HMO with aggregate claims information. Under the rule, the plan sponsor can obtain summary information with certain identifiers removed, in order to provide it to the HMO and receive a premium rate.

The Department assumes that most plan sponsors who are small employers (those with 50 or fewer employees) will elect not to receive protected health information because they will have little, if any, need for such data. Any needs that plan sponsors of small group health plans may have for information can be accomplished by receiving the information in summary form. The Department has assumed that only 5 percent of plan sponsors of small group health plans that provide coverage through a contract with an issuer will actually take the steps necessary to receive protected health information. This is approximately 96,900 firms. For these firms, the Department assumes it will take one hour to determine procedural and organization issues and an additional ⅓ hour of an attorney's time to make plan document changes, which will be simple and essentially standardized. This will cost $7.1 million.

Plan sponsors who are employers of medium (51–199 employees) and large (over 200 employees) firms that provide health benefits through contracts with issuers are more likely to want access to protected health information for plan administration, for example to use it to audit claims or perform quality assurance functions on behalf of the group health plan. The Department assumes that 25 percent of plan sponsors of medium sized firms and 75 percent of larger firms will want to receive protected health information. This is approximately 38,000 medium size firms and 27,000 larger firms. To provide access to protected health information by the group health plan, a plan sponsor will have to assess the current flow of protected health information from their issuer and determine what information is necessary and appropriate. The plan sponsors may then have to make internal organizational changes to assure adequate protection of protected health information so that the relevant requirements are met for the group health plan. We assume that medium size firms will take 16 work hours to complete organizational changes, plus one hour of legal time to make changes to plan documents and certify to the insurance carrier that the firm is eligible to receive protected health information. We assume that larger firms will require 32 hours of internal organizational work and one hour of legal time. This will cost $52.4 million and is a one-time expense.

Business Associates

The final rule requires a covered entity to have a written contract or other arrangement that documents satisfactory assurance that business associate will appropriately safeguard protected health information in order to disclose it to a business associate based on such an arrangement. The Department expects business associate contracts to be fairly standardized, except for language that will have to be tailored to the specific arrangement between the parties, such as the allowable uses and disclosures of information. The Department assumes the standard language initially will be developed by trade and professional associations for their members. Small providers are likely to simply adopt the language or make minor modifications, while health plans and hospitals may start with the prototype language but may make more specific changes to

meet their institutional needs. The regulation includes a requirement that the covered entity take steps to correct, and in some cases terminate, a contract, if necessary, if they know of violations by a business associate. This oversight requirement is consistent with standard oversight of a contract.

The Department could not derive a per entity cost for this work directly. In lieu of this, we have assumed that the trade and professional associations' work plus any minor tailoring of it by a covered entity would amount to one hour per non-hospital provider and two hours for hospitals and health plans. The larger figure for hospitals and health plans reflects the fact that they are likely to have a more extensive array of relationships with business associates.

The cost for the changes in business associate contracts is estimated to be $103 million. This will be an initial year cost only because the Department assumes that this contract language will become standard in future contracts.

In addition, the Department has estimated the cost for business associates to comply with the minimum necessary provisions. As part of the minimum necessary provisions, covered entities will have to establish policies to ensure that only the minimum necessary protected health information is shared with business associates. To the extent that data are exchanged, covered entities will have to review the data and systems programs to assure compliance.

For non-hospital providers, we estimate that the first year will require an average of three hours to review existing agreements, and thereafter, they will require an additional hour to assure business associate compliance. We estimate that hospitals will require an additional 200 hours the first year and 16 hours in subsequent years; health plans will require an additional 112 hours the first year and 8 hours in subsequent years. As in other areas, we have assumed a weighted average wage for the respective sectors.

The cost of the covered entities assuring business associates' complying with the minimum necessary is $197 million in the first year, and a total of $697 million over ten years. (These estimates include the both the cost for the covered entity and the business associates.)

Inspection and Copying

In the NPRM estimate, inspection and copying were a major cost. Based on data and information from the public comments and further fact-finding, however, the Department has re-estimated these policies and found them to be much less expensive.

The public comments demonstrate that copying of records is wide-spread today. Records are routinely copied, in whole or in part, as part of treatment or when patients change providers. In addition, copying occurs as part of legal proceedings. The amount of inspection and copying of medical records that occurs for these purposes is not expected to change measurably as a result of the final regulation.

The final regulation establishes the right of individuals to access, that is to inspect and obtain a copy of, protected health information about them in designated record sets. Although this is an important right, the Department does not expect it to result in dramatic increases in requests from individuals. 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, we assumed that most providers currently have procedures for allowing patients to inspect and obtain a copy of individually identifiable health information about themselves. The economic impact of requiring entities to allow individuals to access their records should be relatively small. One public commenter addressed this issue and provided specific data which supports this conclusion.

Few studies address the cost of providing medical records to patients. The most recent was a study in 1998 by the Tennessee Comptroller of the Treasury. It found an average cost of $9.96 per request, with an average of 31 pages per request. The 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 have more complicated records than those in a primary care or other types of offices. 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).

In estimating the cost of copying records, the Department relied on the public comment from a medical records outsourcing industry representative, which submitted specific volume and cost data from a major firm that provides extensive medical record copying services. According to these data, 900 million pages of medical records are copied each year in the U.S., the average medical record is 31 pages, and copying costs are $0.50 per page. In addition, the commenter noted that only 10 percent of all requests are made directly from patients, and of those, the majority are for purposes of continuing care (transfer to another provider), not for purposes of individual inspection. The Department assumed that 25 percent of direct patient requests to copy medical records are for purposes of inspecting their accuracy (i.e., 2.5 percent of all copy requests) or 850,000 in 2003 if the current practice remained unchanged.

To estimate the marginal increase in copying that might result from the regulation, the Department assumed that as patients gained more awareness of their right to inspect and copy their records, more requests will occur. As a result, the Department assumed a ten percent increase in the number of requests to inspect and copy medical records over the current baseline, which would amount to a little over 85,000 additional requests in 2003 at a cost of $1.3 million. Allowing for a 5.3 percent increase in records based on the increase in ambulatory care visits, the highest growth rate among health service sectors (the National Ambulatory Medical Care Survey, 1998), the total cost for the ten-year period would be $16.8 million.

The final rule allows a provider to deny an individual the right to inspect or obtain a copy of protected health information in a designated record set under certain circumstances, and it provides, in certain circumstances, that the patient can request the denial to be reviewed by another licensed health care professional. The initial provider can choose a licensed health care professional to render the second review.

The Department assumes denials and subsequent requests for reviews will be extremely rare. The Department estimates there are about 932,000 annual requests for inspections (*i.e.,* base plus new requests resulting from the regulation), or approximately 11 million over the ten-year period. If one-

tenth of one percent of these requests were to result in a denial in accordance with the rule, the result would be 11,890 cases. Not all these cases would be appealed. If 25 percent were appealed, the result would be 2,972 cases. If a second provider were to spend 15 minutes reviewing the case, the cost would be $6,000 in the first year and $86,360 over ten years.

Amendments to Protected Health Information

Many providers and health plans currently allow patients to amend the information in their medical record, where appropriate. If an error exists, both the patient and the provider or health plan benefit from the correction. However, as with inspection and copying, many states do not provide individuals with the right to request amendment to protected health information about themselves. Based on these assumptions, the Department concludes that the principal economic effect of the final rule would be to expand the right to request amendments to protected health information held by a health plan or provider to those who are not currently covered by amendment requirements under state laws or codes of conduct. In addition, the rule may draw additional attention to the issue of inaccuracies in information and may stimulate patient demand for amendment of medical records, including in those states that currently provide a right to amend medical records.

Under the final regulation, if a patient requests an amendment to his or her medical record, the provider must either accept the amendment or provide the individual with the opportunity to submit a statement disagreeing with the denial. The provider must acknowledge the request and inform the patient of his action.

The cost calculations assume that individuals who request an opportunity to amend their medical record have already obtained a copy of it. Therefore, the administrative cost of amending the patient's record is completely separate from inspection and copying costs.

Based on fact-finding discussions with a variety of providers, the Department assumes that 25 percent of the projected 850,000 people who request to inspect their records will seek to amend them. This number is the existing demand plus the additional requests resulting from the rule. Over ten years, the number of expected amendment requests will be 2.7 million. Unlike inspections, which currently occur in a small percentage of cases, our fact-finding suggests that patients very rarely seek to amend their records, but that the establishment of this right in the rule will spur more requests. The 25 percent appears to be high based on our discussions with providers but it is being used to avoid an underestimation of the cost.

As noted, the provider or health plan is not required to evaluate any amendment requests, only to append or otherwise link to the request in the record. We expect the responses will vary: sometimes an assistant will only make the appropriate notation in the record, requiring only a few minutes; other times a provider or manager will review the request and make changes if appropriate, which may require as much as an hour. To be conservative in its estimate, the Department has assumed, on average, 30 minutes for each amendment request at a cost of $47.28 per hour (2000 CPS).

The first-year cost for the amendment policy is estimated to be $5 million. The ten-year cost of this provision is $78.8 million.

Law Enforcement and Judicial and Administrative Proceedings

The law enforcement provisions of the final rule allow disclosure of protected health information without patient authorization under four circumstances: (1) Pursuant to legal process or as otherwise required by law; (2) to locate or identify a suspect, fugitive, material witness, or missing person; (3) under specified conditions regarding a victim of crime; and (4) and when a covered entity believes the protected health information constitutes evidence of a crime committed on its premises. As under current law and practice, a covered entity may disclose protected health information to a law enforcement official if such official.

Based on our fact finding, we are not able to estimate any additional costs from the final rule regarding disclosures to law enforcement officials. The final rule makes clear that current court orders and grand jury subpoenas will continue to provide a basis for covered entities to disclose protected health information to law enforcement officials. The three-part test, which covered entities must use to decide whether to disclose information in response to an administrative request such as an administrative subpoena, represents a change from current practice. There will be only minimal costs to draft the standard language for such subpoenas. We are unable to estimate other costs attributable to the use of administrative subpoenas. We have not been able to discover any specific information about the costs to law enforcement of establishing the predicates for issuing the administrative subpoena, nor have we been able to estimate the number of such subpoenas that will likely be issued once the final rule is implemented.

A covered entity may disclose protected health information in response to an order in the course of a judicial or administrative proceeding if reasonable efforts have been made to give the individual, who is the subject of the protected health information, notice of and an opportunity to object to the disclosure or to secure a qualified protective order.

The Department was unable to estimate any additional costs due to compliance with the final rule's provisions regarding judicial and administrative proceedings. The provision requiring a covered entity to make efforts to notify an individual that his or her records will be used in proceedings is similar to current practice; attorneys for plaintiffs and defendants agreed that medical records are ordinarily produced after the relevant party has been notified. With regard to protective orders, we believe that standard language for such orders can be created at minimal cost. The cost of complying with such protective orders will also likely be minimal, because attorney's client files are ordinarily already treated under safeguards comparable to those contemplated under the qualified protective orders. The Department was unable to make an estimate of how many such protective orders might be created annually.

We thus do not make any estimate of the initial or ongoing costs for judicial, administrative, or law enforcement proceedings.

Costs to the Federal Government

The rule will have a cost impact on various federal agencies that administer programs that require the use of individual health information. The federal costs of complying with the regulation and the costs when federal government entities are serving as providers are included in the regulation's total cost estimate outlined in the impact analysis. Federal agencies or programs clearly affected by the rule are those that meet the definition of a covered entity. 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 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 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 and standards set by the Departments and implemented through their contracts with providers, this rule is nonetheless expected to create additional requirements. Further, we anticipate that most federal health programs will, to some extent, need to modify their existing practices to comply fully with this rule. The cost to federal programs that function as health plans will be generally the same as those for the private sector.

A unique cost to the federal government will be in the area of enforcement. The Office for 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 may have additional costs to the federal government through increased litigation, appeals, and inspector general oversight.

Examples of other unique costs to the federal government may include such activities as public health surveillance at the Centers for Disease Control and Prevention, health research projects at the Agency for Healthcare Research and Quality, 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.

We estimate that federal costs under this rule will be approximately $196 million in 2003 and $1.8 billion over ten years. The ten-year federal cost estimate represents about 10.2 percent of the privacy regulation's total cost. This estimate was derived in two steps.

First, we assumed that the proportion of the privacy regulation's total cost accruing to the federal government in a given year will be equivalent to the proportion of projected federal costs as a percentage of national health expenditures for that year. To estimate these proportions, we used the Health Care Financing Administration's November 1998 National Health Expenditure projections (the most recent data available) of federal health expenditures as a percent of national health expenditures from 2003 through 2008, trended forward to 2012. We then adjusted these proportions to exclude Medicare and Medicaid spending, reflecting the fact that the vast majority of participating Medicare and Medicaid providers will not be able to pass through the costs of complying with this rule to the federal government because they are not reimbursed under cost-based payment systems. This calculation yields a partial federal cost of $166 million in 2003 and $770 million over ten years.

Second, we add the Medicare and federal Medicaid costs resulting from the privacy regulation that HCFA's Office of the Actuary project can be passed through to the federal government. These costs reflect the actuaries' assumption regarding how much of the total privacy regulation cost burden will fall on participating Medicare and Medicaid providers, based on the November 1998 National Health Expenditure data. Then the actuaries estimate what percentage of the total Medicare and federal Medicaid burden could be billed to the programs, assuming that (1) only 3 percent of Medicare providers and 5 percent of Medicaid providers are still reimbursed under cost-based payment systems, and (2) over time, some Medicaid costs will be incorporated into the state's Medicaid expenditure projections that are used to develop the federal cost share of Medicaid spending. The results of this actuarial analysis add another $30 million in 2003 and $1.0 billion over ten years to the federal cost estimate. Together, these three steps constitute the total federal cost estimate of $236 million in 2003 and $2.2 billion over ten years.

Costs to State and Local Governments

The rule will also have a cost effect on various state and local agencies that administer programs requiring the use of individually identifiable health information. State and local 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 individually identifiable health 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 and local agencies or programs encompassed by the broad scope of this rule include: Medicaid, State Children's Health Insurance Programs, county hospitals, state mental health facilities, state or local nursing facilities, local health clinics, and public health surveillance activities, among others. We have included state and local costs in the estimation of total costs in this section.

The greatest cost and administrative burden on the state and local government will fall to agencies and programs that act as covered entities, by virtue of being either a health plan or provider, such as Medicaid, State Children's Health Insurance Programs, and county hospitals. These and other health insurance or provider programs operated by state and local government are subject to requirements placed on covered entities under this rule, including, but not limited to, those outlined in this section (Section E) of the impact analysis. Many of these state and local programs already afford privacy protections for individually identifiable health information through the Privacy Act. For example, state governments often become subject to Privacy Act requirements when they contract with the federal government. This rule is expected to create additional requirements beyond those covered by the Privacy Act. Furthermore, we anticipate that most state and local health programs will, to some extent, need to modify their existing Privacy Act practices to fully comply with this rule. The cost to state

and local programs that function as health plans will be different than the private sector, much as the federal costs vary from private health plans.

A preliminary analysis suggests that state and local government costs will be on the order of $460 million in 2003 and $2.4 billion over ten years. We assume that the proportion of the privacy regulation's total cost accruing to state and local governments in a given year will be equivalent to the proportion of projected state and local costs as a percentage of national health expenditures for that year. To estimate these proportions, we used the Health Care Financing Administration's November 1998 National Health Expenditure projections of state and local health expenditures as a percent of national health expenditures from 2003 through 2008, trended forward to 2012. Based on this approach, we assume that over the entire 2003 to 2012 period, 13.6 percent, or $2.4 billion, of the privacy regulation's total cost will accrue to state and local governments. Of the $2.4 billion state and local government cost, 19 percent will be incurred in the regulation's first year (2003). In each of the out-years (2004–2012), the average percent of the total cost incurred will be about nine percent per year. These state and local government costs are included in the total cost estimates discussed in the regulatory impact analysis.

F. Benefits

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.[52] 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. Therefore, 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 security that individuals feel when personal information is kept confidential. This benefit is very real and very significant but there are no reliable means of measuring dollar value of such benefit.

As noted in the comment and response section, a number of commenters raised legitimate criticisms of the Department's approach to estimating benefits. The Department considered other approaches, including attempts to measure benefits in the aggregate rather than the specific examples set forth in the NPRM. However, we were unable to identify data or models that would provide credible measures. Privacy has not been studied empirically from an economic perspective, and therefore, we concluded that the approach taken in the NPRM is still the most useful means of illustrating that the benefits of the regulation are significant in relation to the economic costs.

Before beginning the 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 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 (the most recent available at the time of the analysis), which show that 220 million persons are covered by either private or public health insurance. Joining the Census Bureau data with the costs calculated in Section E, we have estimated the cost of the regulation to be approximately $6.25 per year (or approximately $0.52 per month) for each insured individual (including people in government programs). If we assume that individuals who use the health care system will be willing to pay more than this per year 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 or are in government programs will use medical services or benefit from the provisions of the proposed regulation. Currently, there are 42 million Americans who do not have any form of health care coverage. 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 possible cost for 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 Healthcare Policy Research (AHCPR) show approximately 776.3 million health care visits (*e.g.,* office visits, hospital and nursing home stays, etc.) in the first year (2003). As with the calculation of average annual cost per insured patient, we divided the total cost of complying with the regulation by the total annual number of health care visits. The cost of instituting requirements of the proposed regulation is $0.19 per health care visit. If we assume that individuals would be willing to pay more than $0.19 per health care visit to improve health information privacy, the benefits of the proposed regulation 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.'' [53] 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.'' [54] These concerns would be partly allayed by the privacy standard.

Fear of disclosure of treatment is an impediment to health care for many Americans. In the 1993 Harris-Equifax Health Information Privacy Survey, seven 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 two percent reported having chosen not to file an insurance claim because of concerns of lack of privacy or confidentiality.[55] Increased confidence

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

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

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

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

on the part of patients that their privacy would be protected would lead to increased 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). It will also change the dynamic of current payments. Insured patients currently paying out-of-pocket to protect confidentiality will be more likely to file with their insurer and to seek all necessary care. The increased utilization that would result from increased confidence in privacy could be beneficial under many circumstances. For many medical conditions, early and comprehensive treatment can lead to lower costs.

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, including relatively minor conditions. We expect that some individuals might be concerned with maintaining privacy even if they have no significant health problems because it is likely that they will develop a medical condition in the future that they will 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,[56] exceeded only by heart disease. In 2000, it is estimated that 1.22 million new cancer cases will be diagnosed.[57] The estimated prevalence of cancer cases (both new and existing cases) in 1999 was 8.37 million.[58] In addition to mortality, incidence, and prevalence rates, the other primary methods of assessing the burden of disease are cost-of-illness and quality of life measures.[59] Cost of illness measures the economic costs associated with treating the disease (direct costs) and lost income associated with morbidity and mortality (indirect costs). The National Institutes of Health estimates that the overall annual cost of cancer in 1990 was $96.1 billion; $27.5 billion in direct medical costs and $68.7 billion for lost income due to morbidity and mortality.[60] Health-related quality of life measures integrate the mortality and morbidity effects of disease to produce health status scores for an individual or population. For example, the Quality Adjusted Life Year (QALY) combines the pain, suffering, and productivity loss caused by illness into a single measure. The Disability Adjusted Life Year (DALY) is based on the sum of life years lost to premature mortality and years that are lived, adjusted for disability.[61] The analysis below is based on the cost-of-illness measure for cancer, which is more developed than the quality of life measure.

Among the most important elements in the fight against cancer are screening, early detection and treatment of the disease. However, many patients are concerned that cancer detection and treatment 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 treatment, cancer patients may ultimately face a more severe illness and/or premature death.

Increasing people's confidence in the privacy of their medical information would encourage more people with cancer to seek cancer treatment earlier, which would increase cancer survival rates and thus reduce the lost wages associated with cancer. 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.[62]

We have attempted to estimate the annual savings in foregone wages that would result from earlier treatment due to enhanced protection of the privacy of medical records. We do not assume there would be increased medical costs from earlier treatment because the costs of earlier and longer cancer treatment are probably offset by the costs of treating late-stage cancer among people who would otherwise not be treated until their cases had progressed.

Although figures on the number of individuals who avoid cancer 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 seven 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 affirmatively. However, for the purposes of this estimate, we assume that privacy concerns were responsible for the majority of positive responses.

Based on the Harris-Equifax survey estimate that seven percent of people did not seek services for physical or mental health conditions due to fears about job prospects or other opportunities, we assume that the proportion of people diagnosed with cancer who did not seek earlier treatment due to these fears is also seven percent. Applying this seven percent figure to the estimated number of total cancer cases (8.37 million) gives us an estimate of 586,000 people who did not seek earlier cancer treatment due to privacy concerns. We estimate annual lost wages due to cancer morbidity and mortality per cancer patient by dividing total lost wages ($68.7 billion) by the number of cancer patients (8.37 million), which rounds to $8,200. We then assume that cancer patients who seek earlier treatment would achieve a one-third reduction in cancer mortality and morbidity due to earlier treatment. The assumption of a one-third reduction in mortality and morbidity is derived from a study showing a one-third reduction in colorectal cancer mortality due to colorectal cancer screening.[63] We could have chosen a lower or higher treatment success rate. By multiplying 586,000 by $8,200 by one-third, we calculate that $1.6 billion in lost wages could be saved each year by encouraging more people to seek early cancer treatment through enhanced privacy protections. This estimate illustrates the potential savings

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

[57] American Cancer Society. http://www3.cancer.org/cancerinfo/sitecenter.asp?ctid=8&scp= 0&scs= 0&scss= 0&scdoc = 40000.

[58] Polednak, AP. ''Estimating Prevalence of Cancer in the United States,'' Cancer 1997; 8–:136–41

[59] Martin Brown, ''The Burden of Illness of Cancer: Economic Cost and Quality of Life.'' Annual Review of Public Health, 2001:22:91–113.

[60] Disease-Specific Estimates of Direct and Indirect Costs of Illness and NIH Support: Fiscal Year 2000 Update. Department of Health and Human Services, Naitonal Institutes of Health, Office of the Director, February 2000.

[61] DALY scores for 10 cancer sites are presented in Brown, ''The Burden of Illness of Cancer: Economic Cost and Quality of Life,'' figure 1.

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

[63] Jack S. Mandel, *et al.,* ''Reducing Mortality from Colorectal Cancer by Screening for Fecal Occult Blood,'' The New England Journal of Medicine, May 13, 1993, Vol, 328, No. 19.

in lost wages due to cancer that could be achieved with greater privacy protections.

HIV/AIDS

Early detection is essential for the survival of a person with HIV (Human Immunodeficiency Virus). Concerns about the confidentiality of HIV status would likely deter some people from getting tested. For this reason, each state has passed some sort of legislation regarding confidentiality of an individual's 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.[64] 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.[65] 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 of early HAART treatment is estimated at $23,700 per quality-adjusted year of life saved.[66]

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.[67] For a potentially embarrassing disease such as an STD, seeking treatment requires trust in both the provider and the health care system for confidentiality of such information. 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.[68] In addition, there could be greater overall savings if earlier treatment translates into reduced spread of infections.

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 mental health treatment. One way that individuals will receive this information is through the notice requirement. Increased use of mental health and services would be expected to be beneficial to the persons receiving the care, to their families, and to society at large. The direct benefit to the individual from treatment would include improved quality of life, reduced disability associated with mental conditions, reduced mortality rate, and increased productivity associated with reduced disability and mortality. 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 potential economic benefits associated with improving privacy of individually identifiable health information and thus encouraging some portion of individuals to seek initial mental health treatment or increase service use are difficult to quantify well. Nevertheless, using a methodology similar to the one used above to estimate potential savings in cancer costs, one can lay out a range of possible benefit levels to illustrate the possibility of cost savings associated with an expansion of mental health and treatment to individuals who, due to protections offered by the privacy regulation, might seek treatment that they otherwise would not have. This can be illustrated by drawing upon existing data on the economic costs of mental illness and the treatment effectiveness of interventions.

The 1998 Substance Abuse and Mental Health Statistics Source Book from the Substance Abuse and Mental Health Services Administration (SAMHSA) estimates that the economic cost to society of mental illness in 1994 was about $204.4 billion. About $91.7 billion was due to the cost of treatment and medical care and $112.6 billion (1994 dollars) was due to loss of productivity associated with morbidity and mortality and other related costs, such as crime.[69] 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 millions of dollars in cost savings annually.

Although figures on the number of individuals who avoid mental health treatment due to privacy concerns do not exist, some indirect evidence is available. As noted in the cancer discussion, the 1993 Harris-Equifax Health Information Privacy Survey 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. (See above for limitations to this data).

We assume that the proportion of people with a mental health disorder who did not seek treatment due to fears about job prospects or other opportunities is the same as the proportion in the Harris-Equifax survey sample who did not seek services for physical or mental health conditions due to the same fears (7 percent). The 1999 Surgeon General's Report on Mental Health estimates that 28 percent of the U.S. adult population has a diagnosable mental and/or substance abuse disorder and 20 percent of the population has a mental and/or substance abuse disorder for which they do not receive treatment.[70] Based on the Surgeon General's Report, we estimate that 15 percent of the adult population has a mental disorder for which they do not seek treatment.[71] Assuming that 7

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

[65] 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.

[66] 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.

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

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

[69] Substance Abuse and Mental Health Services Administration. *http://www.samhsa.gov/oas/srcbk/costs-02htm.* Source of data: DP Rice, Costs of Mental Illness (unpublished data).

[70] Department of Health and Human Services, Mental Health: A Report of the Surgeon General. Rockville, MD: 1999, page 408.

[71] According to the Surgeon General's Report, 28 percent of the adult population have either a mental or addictive disorder, whether or not they receive services: 19 percent have a mental disorder alone, 6 percent have a substance abuse disorder alone, and 3 percent have both. Subtracting the 3 percent who have both, about three-quarters of the population with either a mental or addictive disorder have a mental disorder and one-quarter have a substance abuse disorder. We assume that this ratio (three-quarter to one-quarter) is the same for the adult population with either a mental or addictive disorder who do not receive services.

percent of those with mental disorders did not seek treatment due to privacy concerns, we estimate that 1.05 percent of the adult population [72] (15 percent multiplied by 7 percent), or 2.07 million people, did not seek treatment for mental illness due to privacy fears.

The indirect (non-treatment) economic cost of mental illness per person with mental illness is $2,590 ($112.6 billion divided by 43.4 million people with mental illness).[73] The treatment cost of mental illness per person with mental illness is $2,110 ($91.7 billion divided by 43.4 million individuals). If we assume that indirect economic costs saved by encouraging more individuals with mental illness to enter treatment are offset by the additional treatment costs, the net savings is about $480 per person.

As stated above, appropriate treatment of mental health disorders can result in 50-80 percent of individuals experiencing improvements in these types of conditions. Therefore, we multiply the number of individuals with mental disorders who would seek treatment with greater privacy protections (2.07 million) by the treatment effectiveness rate by the net savings per effective treatment ($480). Assuming a 50 percent success rate, this equation yields annual savings of $497 million. Assuming an 80 percent success rate, this yields annual savings of $795 million.

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 would seek mental health treatment with greater privacy protections, the potential net economic benefits could range from approximately $497 million to $795 million annually.

V. Final Regulatory Flexibility Analysis

A. Introduction

Pursuant to the Regulatory Flexibility Act 5 U.S.C. 601 *et seq.,* the Department must prepare a regulatory flexibility analysis if the Secretary certifies that a final rule would have a significant economic impact on a substantial number of small entities.[74]

This analysis addresses four issues: (1) The need for, and objective of, the rule; (2) a summary of the public comments to the NPRM and the Department's response; (3) a description and estimate of the number of small entities affected by the rule; and (4) a description of the steps the agency has taken to minimize the economic impact on small entities, consistent with the law and the intent of the rule. The following sections provide details on each of these issues. A description of the projected reporting and record keeping requirements of the rule are included in Section IX, below.

B. Reasons for Promulgating the Rule

This proposed rule is being promulgated in response to a statutory mandate 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 (see Section I. B. above).

1. Objectives and Legal Basis

This information can be found in earlier preamble discussions (See I. C. and IV., above).

2. Relevant Federal Provisions

This information can be found in earlier preamble discussions (See I. C., above).

C. Summary of Public Comments

The Department received only a few comments regarding the Initial Regulatory Flexibility Analysis (IRFA) contained in the NPRM. A number of commenters argued that the estimates IRFA were too low or incomplete. The estimates were incomplete to the extent that a number of significant policy provisions in the proposal were not estimated because of too little information at the time. In the final IRFA we have estimates for these provisions. As for the estimates being too low, the Department has sought as much information as possible. The methodology employed for allocating costs to the small business sectors is explained in the following section.

Most of the other comments pertaining to the IRFA criticized specific estimates in the NPRM. Generally, the commenters argued that certain cost elements were not included in the cost estimates presented in the NPRM. The Department has expanded our description of our data and methodology in both the final RIA and this final RFA to try to clarify the data and assumptions made and the rationale for using them.

Finally, a number of commenters suggested that small entities be exempted from coverage from the final rule, or that they be given more time to comply. As the Department has explained in the Response to Comment section above, such changes were considered but rejected. Small entities constitute the vast majority of all entities that are covered; to exempt them would essentially nullify the purpose of the rule. Extensions were also considered but rejected. The rule does not take effect for two years, which is ample time for small entities to learn about the rule and make the necessary changes to come into compliance.

D. Economic Effects on Small Entities

1. Number and Types of Small Entities Affected

The Small Business Administration defines small businesses in the health care sector as those organizations with less than $5 million in annual revenues. Nonprofit organizations are also considered small entities;[75] 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.[76]

Small business in the health care sector affected by this rule may include such businesses as: Nonprofit health plans, hospitals, and skilled nursing facilities (SNFs); small businesses providing health coverage; small physician practices; pharmacies; laboratories; 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 1997, there were 562,916 small health care entities [77] classified within the SIC

Thus, we assume that 15 percent of the population have an untreated mental disorder (three-quarters of 20 percent) and 5 percent have an untreated addictive disorder (one-quarter of 20 percent).

[72] According to the Population Estimates Program, Population Division, U.S. Census Bureau, the U.S. population age 20 and older is 197.1 million on Sept. 1, 2000. This estimate of the adult population is used throughout this section.

[73] The number of adults with mental illness is calculated by multiplying the U.S. Census Bureau estimate of the U.S. adult population—197.1 million—by the percent of the adult population with mental illness—22 percent, according to the Surgeon General's Report on Mental Health, which says that 19 percent of the population have a mental disorder alone and three percent have a mental and substance abuse disorder.

[74] ''Entities'' and ''establishments'' are synonymous in this analysis.

[75] ''Entities'' and ''establishments'' are used synonymously in this RFA.

[76] ''Small governments'' were not included in this analysis directly; rather we have included the kinds of institutions within those governments that are likely to incur costs, such as government hospitals and clinics.

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

codes we have identified as being covered establishments (Table A).

Table A.--Number of Health Care Establishments That Meet SBA Size Standards, 1997[1]

Standard Industrial Code (SIC)	Industry	Total Number of Health Care Establishments	Number of Establishments that Meet SBA Size Standards[2] or RFA non- profit standard	% of Establishments that Meet SBA Size Standards[2] or RFA non-profit standard
5910	Drug Stores & Proprietary Stores	48,147	23,923	49.7%
6320	Accident & Health Insurance & Medical Service Plans	8,083	665	8.2%
7352	Medical Equipment Rental and Leasing	3,346	1,836	54.9%
8010	Offices & Clinics Of Doctors Of Medicine	190,233	170,962	89.9%
8020	Offices & Clinics Of Dentists	115,020	113,864	99.0%
8030	Offices & Clinics Of Doctors Of Osteopathy	9,143	8,850	96.8%
8040	Offices & Clinics Of Other Health Practitioners	89,482	86,596	96.8%
8050	Nursing & Personal Care Facilities	33,178	17,727	53.4%
8060	Hospitals	6,991	3,485	49.8%
8070	Medical & Dental Laboratories	17,586	13,015	74.0%
8080	Home Health Care Services	19,562	12,841	65.6%
8090	Miscellaneous Health & Allied Services	22,145	11,219	50.7%
n/a	Fully Insured ERISA[2]	2,125,000	0	NA
n/a	Institutional Review Boards (IRB)[2]	450,000	0	NA
n/a	Total[2]	562,916	464,983	82.6%

1 Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997. Establishments that have less than $5,000,000 in annual revenue are considered small businesses here, as are non-profit establishments (regardless of revenue). We have non-profit data for the following SICs: 8050, 8060, and 8080 and have included the number of non-profits in each category into the table.

[2] We have not included the number of fully insured ERISA plans or institutional review boards (IRB) in the total number of health care establishments or the number of establishments that meet SBA standards for small entities, since these are not separate businesses with SIC codes and we do not have sufficient data to impute revenues to them.

[3] We have included self-insured, self-administered plans and third party administrators in the total number of health plans, even though neither has individual SIC codes because we have the ability to impute revenues to them. Therefore, the number of health plans in SIC 6320 is greater than the figure usually reported in the Statistics of U.S. Businesses.

These small businesses represent 82.6% of all health care establishments examined.[78] Small businesses represent a significant portion of the total number of health care establishments but a small portion of the revenue stream for all health care establishments. In 1997, the small health care businesses represented generated approximately $430 billion in annual receipts, or 30.2% of the total revenue generated by health care establishments (Table B).[79] The following sections provide estimates of the number of small health care establishments that will be required to comply with the rule. Note, however, that the SBA's published annual receipts of health care industries differ from the National Health Expenditure data that the Health Care Financing Administration (HCFA) maintains.

[78] Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997.

[79] Op.cit, 1997.

These data do not provide the specific revenue data required for a RFA; only the SBA data has the requisite establishment and revenue data for this analysis.

Table B.--Annual Receipts of Health Care Entities, 1997[1]

Standard Industrial Code (SIC)	Industry	Total Revenue	Revenue Generated by Small Entities	% of Total Revenue Generated by Small Entities
5910	Drug Stores & Proprietary Stores	$100,302,441,000	$25,620,978,000	25.5%
6320	Accident & Health Insurance & Medical Service Plans (SIC 6320), Self-Insured/ Self Administered (no SIC), Third Party Administrators (no SIC)2	$512,111,493,027	$657,074,000	0.1%
7352	Medical Equipment Rental & Leasing	$4,040,646,000	$1,193,345,000	29.5%
8010	Offices & Clinics Of Doctors Of Medicine	$182,148,148,000	$105,334,031,000	57.8%
8020	Offices & Clinics Of Dentists	$48,766,434,000	$47,218,844,000	96.8%
8030	Offices & Clinics Of Doctors Of Osteopathy	$4,613,192,000	$4,039,868,000	87.6%
8040	Offices & Clinics Of Other Health Practitioners	$28,110,189,000	$23,170,899,000	82.4%
8050	Nursing & Personal Care Facilities	$77,166,537,000	$24,484,098,431	31.7%
8060	Hospitals	$382,540,791,000	$172,552,388,454	45.1%
8070	Medical & Dental Laboratories	$19,872,150,000	$6,862,628,000	34.5%
8080	Home Health Care Services	$31,061,036,000	$12,085,755,906	38.9%
8090	Miscellaneous Health & Allied Services	$35,034,774,000	$6,812,006,000	19.4%
N/A	Total Receipts	$1,425,767,831,027	$430,031,915,791	30.2%

1 Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997. Entities that have less than $5,000,000 in annual revenue are considered small businesses here, as are non-profit entities (regardless of revenue). We have non-profit data for the following SICs: 8050, 8080, and 8060 and have included the number of non-profits in each category into the table.

2 We have included self-insured/self-administered plans and third party administrators in the total number of health plans, even though neither has individual SIC codes because we have the ability to impute revenues to them.

The Small Business Administration reports that approximately 74 percent of the 18,000 medical laboratories and dental laboratories in the U.S. are small entities.[80] Furthermore, based on SBA data, 55 percent of the 3,300 durable medical equipment suppliers that are not part of drug and proprietary stores in the U.S. are small entities. Over 90 percent of health practitioner offices are small businesses.[81] Doctor offices (90%), dentist offices (99%), osteopathy (97%) and other health practitioner offices (97%) are primarily considered small businesses.

There are also a 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. and the Health Care Financing Administration reports that there are 591 nonprofit nursing facilities and 4,280 nonprofit skilled nursing facilities.[82]

Some contractors that are not covered entities but that work with covered 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.

2. Activities and Costs Associated With Compliance

This section summarizes specific activities that covered entities must undertake to comply with the rule's provisions and options considered by the Department that would reduce the burden to small entities. In developing this rule, the Department considered a variety of alternatives for minimizing the economic burden that it will create for small entities. We did not exempt small businesses from the rule because they represent such a large and critical proportion of the health care industry (82.6 percent); a significant portion of individually identifiable health information is generated or held by these small businesses.

The guiding principle in our considerations of how to address the burden on small entities has been to make provisions performance rather than specification oriented—that is, the rule states the standard to be achieved but allows institutions flexibility to determine how to achieve the standard within certain parameters. Moreover, to the extent possible, we have allowed entities to determine the extent to which they will address certain issues. This ability to adapt provisions to minimize burden has been addressed in the regulatory impact analysis above, but it 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 rule. The Department considered extending the compliance period for small entities but concluded that it did not have the legal authority to do so (see discussion above). The rule, pursuant to HIPAA, creates an extended compliance time of 36 months (rather than 24 months) only for small health plans and not for other small entities. The Department also considered giving small entities longer response times for time limits set forth in the rule, but decided to establish standard time limits that we believe are reasonable for covered entities of all sizes, with the understanding that larger entities may not need as much time as they have been allocated in certain situations. This permits each covered entity the flexibility to establish policies regarding time limits that are consistent with the entity's current practices.

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

Scalability

Wherever possible, the final rule provides a covered entity with flexibility to create policies and procedures that are best suited to the entity's current practices in order to comply with the standards, implementation specifications, and requirements of the rule. This allows the covered entity to assess its own needs in devising, implementing, and maintaining appropriate privacy policies, procedures, and documentation to address these regulatory requirements. It also will allow a covered entity to take advantage of developments and methods for protecting privacy that will evolve over time in a manner that is best suited to that institution. This approach allows covered entities to strike a balance between protecting privacy of individually identifiable health information and the economic cost of doing so within prescribed boundaries set forth in the rule. Health care entities must consider both factors when devising their privacy solutions. The Department assumes that professional and trade associations will provide guidance to their members in understanding the rule and providing guidance on how they can best achieve compliance. This philosophy is similar to the approach in the Transactions Rule.

The privacy standard must be implemented by all covered entities, regardless of size. However, we believe that the flexible approach under this rule is more efficient and appropriate then a single approach to 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 of her duties. In a large health plan, the privacy official position may require more time and greater privacy experience, or the privacy official may have the regular support and advice of a privacy staff or board. The entity can decide how to implement this privacy official requirement based on the entity's structure and needs.

The Department decided to use this scaled approach to minimize the burden on all entities, with an emphasis on small entities. The varying needs and capacities of entities should be reflected in the policies and procedures adopted by the organization and the overall approach it takes to achieve compliance.

Minimum Necessary

The ''minimum necessary'' policy in the final rule has essentially three components: first, it does not pertain to certain uses and disclosures including treatment-related exchange of information among health care providers; second, for disclosures that are made on a routine basis, such as insurance claims, a covered entity is required to have policies and procedures governing such exchanges (but the rule does not require a case-by-case determination in such cases); and third, providers must have a process for reviewing non-routine requests on a case-by-case basis to assure that only the minimum necessary information is disclosed. The final rule makes changes to the NPRM that reduce the burden of compliance on small businesses.

Based on public comments and subsequent fact-finding, the Department sought to lessen the burden of this

[80] Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997.

[81] Op.cit., 1997.

[82] Health Care Financing Administration, OSCAR.

provision. The NPRM proposed applying the minimum necessary standard to disclosures to providers for treatment purposes and would have required individual review of all uses of protected health information. The final rule exempts disclosures of protected health information from a covered entity to a health care provider for treatment from the minimum necessary provision and eliminates the case-by-case determinations that would have been necessary under the NPRM. The Department has concluded that the requirements of the final rule are similar to the current practice of most health care providers. For standard disclosure requests, for example, providers generally have established procedures. Under the final rule providers will have to have policies and procedures to determine the minimum amount of protected health information to disclose for standard disclosure requests as well, but may need to review and revise existing procedures to make sure they are consistent with the final rule. For non-routine disclosures, providers have indicated that they currently ask questions to discern how much information should be disclosed. In short, the minimum necessary requirements of this rule are similar to current practice, particularly among small providers.

Policy and Procedures

The rule requires that covered entities develop and document policies and procedures with respect to protected health information to establish and maintain compliance with the regulation. Through the standards, requirements, and implementation specifications, we are proposing a framework for developing and documenting privacy policies and procedures rather than adopting a rigid, prescriptive approach to accommodate entities of different sizes, type of activities, and business practices. Small providers will be able to develop more limited policies and procedures under the rule, than will large providers and health plans, based on the volume of protected health information. We also expect that provider and health plan associations will develop model policies and procedures for their members, which will reduce the burden on small businesses.

Privacy Official

The rule requires covered entities to designate a privacy official who will be responsible for the development and implementation of privacy policies and procedures. The implementation of this requirement may vary based on the size of the entity. For example, a small physician's practice might designate the office manager as the privacy official in addition to her broader administrative responsibilities. Once the privacy official has been trained, the time required to accomplish the duties imposed on such person is not likely to be much more than under current practice. Therefore, the requirement imposes a minimal burden on small businesses.

Internal Complaints

The final rule requires covered entities to have an internal process for individuals to make complaints regarding the covered entities' privacy policies and procedures required by the rule and its compliance with such policies. The requirement includes identifying a contact person or office responsible for receiving complaints and documenting all complaints received and the disposition of such complaints, if any. The covered entity only is required to receive and document a complaint (the complaint can be oral or in writing), which should take a short amount of time. The Department believes that complaints about a covered entity's privacy policies and procedures will be uncommon. Thus, the burden on small businesses should be minimal.

Training

In developing the NPRM, the Department considered a number of alternatives for training, including requiring specific training materials, training certification, and periodic retraining. In the NPRM, the Department recommended flexibility in the materials and training method used, but proposed recertification every three years and retraining in the event of material changes in policy.

Based on public comment, particularly from small businesses, the Department has lessened the burden in the final rule. As in the proposal, the final rule requires all employees who are likely to have contact with protected health information to be trained. Covered entities will have to train employees by the compliance date specific to the type of covered entity and train new employees within a reasonable time of initial employment. In addition, a covered entity will have to train each member of its workforce whose functions are affected by a material change in the policies or procedures of such entity. However, the final rule leaves to the employer the decisions regarding the nature and method of training to achieve this requirement. The Department expects a wide variety of options to be made available by associations, professional groups, and vendors. Methods might include classroom instruction, videos, booklets, or brochures tailored to particular levels of need of workers and employers. Moreover, the recertification requirement of the NPRM has been dropped to ease the burden on small entities.

Consent

The NPRM proposed prohibiting covered entities from requiring individuals to provide written consent for the use and disclosure of protected health information for treatment, payment, and health care operations purposes. The final rule requires certain health care providers to obtain written consent before using or disclosing protected health information for treatment, payment, and health care operations, with a few exceptions. This requirement was included in the final rule in response to comments that this reflects current practice of health care providers health care providers with direct treatment relationships. Because providers are already obtaining such consent, this requirement represents a minimal burden.

Notice of Privacy Rights

The rule requires covered entities to prepare and make available a notice that informs individuals about uses and disclosures of protected health information that may be made by the covered entity and that informs of the individual's rights and covered entity's legal duties with respect to protected health information. The final rule makes changes to the NPRM that reduce the burden of this provision on covered entities and allows flexibility. The NPRM proposed that the notice describe the uses and disclosures of information that the entity *expected to make* without individual authorization. The final rule only requires that the notice describe uses and disclosures that the entity is permitted or required to make under the rule without an individual's written consent or authorization. This change will allow entities to use standardized notice language within a given state, which will minimize the burden of each covered entity preparing a notice. Professional associations may develop model language to assist entities in developing notices required by the rule. While the final rule specifies minimum notice requirements, it allows entities flexibility to add more detail about a covered entity's privacy policies.

The NPRM also proposed that health plans distribute the notice every three years. The final rule reduced this

burden by requiring health plans (in addition to providing notice to individuals at enrollment and prior to the compliance date of this rule) to inform individuals at least once every three years about the availability of the notice and how to obtain a copy rather than to distribute a copy of the notice.

In discussing the requirement for covered entities to prepare and make available a notice, we considered exempting small businesses (83 percent of entities) or extremely small entities (fewer than 10 employees). The Department decided that informing consumers of their privacy rights and of the activities of covered entities with which they conduct business was too important a goal of this rule 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 it would be overly burdensome to all entities, especially small entities, to require two notice.

We believe that the proposed rule appropriately balances the benefits of providing individuals with information about uses and disclosures of protected health information with covered entities' need for flexibility in describing such information.

Access to Protected Health Information

The public comments demonstrate that inspection and copying of individually identifiable health information is wide-spread today. Individuals routinely request copies of such information, in whole or in part, for purposes that include providing health information to another health care provider or as part of legal proceedings. The amount of inspection and copying of individually identifiable health information that occurs for these purposes is not expected to change as a result of the final regulation.

The final regulation establishes the right of individuals to inspect and copy protected health information about them. Although this is an important right, the Department does not expect it to result in dramatic increases in requests from individuals. We assume that most health care providers currently have procedures for allowing patients to inspect and copy this information. The economic impact on small businesses of requiring covered entities to provide individuals with access to protected health information should be relatively small. Moreover, entities can recoup the costs of copying such information by charging reasonable cost-based fees.

Amendments to Protected Health Information

Many health care providers and health plans currently make provisions to help patients expedite amendments and corrections of their medical record where appropriate. If an error exists, both the patient and the health care provider on health plan benefit from the correction. However, as with inspection and copying, a person's right to request amendment and correction of individually identifiable health information about them is not guaranteed by all states. Based on these assumptions, the Department concludes that the principal economic effect of the final rule will be to expand the right to request amendments to protected health information held by health plans and covered health care providers to those who are currently granted such right by state law. In addition, the rule may draw additional attention to the issue of record inaccuracies and stimulate patient demand for amendment of medical records.

Under the final regulation, if an individual requests an amendment to protected health information about him or her, the health care provider must either accept the amendment or provide the individual with the opportunity to submit a statement disagreeing with the denial. We expect the responses to requests will vary; sometimes an assistant will only make the appropriate notation in the record, requiring only a few minutes; other times a health care provider or manager will review the request and make changes if appropriate, which may require as much as an hour.

Unlike inspections, which currently occur in a small percentage of cases, fact-finding suggests that individuals rarely seek to amend their records today, but the establishment of this right in the rule may spur more requests, including among those who in the past would have only sought to inspect their records. Nevertheless, we expect that the absolute number of additional amendment requests caused by the rule to be small (about 200,000 per per spread over more than 600,000 entities), which will impose only a minor burden on small businesses.

Accounting for Disclosures

The rule grants individuals the right to receive an accounting of disclosures made by a health care provider or plan for purposes other than treatment, payment, or health care operations, with certain exceptions such as disclosures to the individual. The individual may request an accounting of disclosures made up to six years prior to the request. In order to fulfill such requests, covered health care providers and health plans may track disclosures by making a notation in the individual's medical record regarding the (manual or electronic) when a disclosure is made. We have learned through fact-finding that some health care providers currently track various types of disclosures. Moreover, the Department does not expect many individuals will request an accounting of disclosures. Thus, this requirement will impose a minor burden on small businesses.

De-Identification of Information

In this rule, the Department allows covered entities to determine that health information is de-identified (*i.e.* that it is not individually identifiable health information), if certain conditions are met. Moreover, information that has been de-identified in accordance with the rule is not considered individually identifiable information and may be used or disclosed without regard to the requirements of the regulation. The covered entity may assign a code or other means of record identification to allow de-identified information to be re-identified if requirements regarding derivation and security are met.

As with other components of this rule, the approach used to remove identifiers from data can be scaled to the size of the entity. Individually identifiable health information can be de-identified in one of two ways; by either removing each of the identifiers listed in the rule or by engaging in a statistical and scientific analysis to determine that information is very unlikely to identify an individual. Small entities without the resources to conduct such an analysis can create de-identified information by removing the full list of possible identifiers set forth in this regulation. Unless the covered entity knows that the information could still identify an individual, the requirement of this rule would be fulfilled. However, larger, more sophisticated covered entities may close to determine independently what information needs to be removed based on sophisticated statistical and scientific analysis.

Efforts to remove identifiers from information are optional. If a covered entity can not use or disclose protected health information for a particular purpose but believes that removing identifiers is excessively burdensome, it can choose not to release the protected health information, or it can seek an authorization from individuals for the use or disclosure of protected health

information including some or all of the identifiers.

Finally, as discussed in the Regulatory Impact Analysis, the Department believes that very few small entities engage in de-identification currently. Fewer small entities are expected to engage in such activity in the future because the increasing trend toward computerization of large record sets will result in de-identification being performed by relatively few firms or associations over time. We expect that a small covered entity will find it more efficient to contract with specialists in large firms to de-identify protected health information. Larger entities are more likely to have both the electronic systems and the volume of records that will make them attractive for this business.

Monitoring Business Associates

The final rule requires a covered entity with a business associate to have a written contract or other arrangement that documents satisfactory assurance that the business associate will appropriately safeguard protected health information. The Department expects business associate contracts to be fairly standardized, except for language that will have to be tailored to the specific arrangement between the parties, such as the allowable uses and disclosures of information. The Department assumes the standard language initially will be developed by trade and professional associations for their members. Small health care providers are likely to simply adopt the language or make minor modifications. The regulation includes a requirement that the covered entity take steps to correct, and in some cases terminate, a contract, if necessary, if they know of violations by a business associate. This oversight requirement is consistent with standard oversight of a contract. The Department expects that most entities, particularly smaller ones, will utilize standard language that restricts uses and disclosures of individually identifiable health information their contracts with business associates. This will limit the burden on small businesses.

The NPRM proposed that covered entities be held accountable for the uses and disclosures of individually identifiable health information by their business associates. An entity would have been in violation of the rule if it knew of a breach in the contract by a business associate and failed to cure the breach or terminate the contract. The final rule reduces the extent to which an entity must monitor the actions of its business associates. The entity no longer has to ''ensure'' that each business associate complies with the rule's requirements. Entities will be required to cure a breach or terminate a contract for business associate actions only if they knew about a contract violation. The final rule is consistent with the oversight a business would provide for any contract, and therefore, the changes in the final rule will impose no new significant cost for small businesses in monitoring their business associates' behavior.

Employers With Insured Group Health Plans

Some group health plans will use or maintain individually identifiable health information, particularly group health plans that are self-insured. Also, some plan sponsors that perform administrative functions on behalf of their group health plans may need protected health information. The final rule permits a group health plan, or a health insurance issuer or HMO that provides benefits on behalf of the group health plan, to disclose protected health information to a plan sponsor who performs administrative functions on its behalf for certain purposes and if certain requirements are met. The plan documents must be amended to: describe the permitted uses and disclosures of protected health information by the plan sponsor; specify that disclosure is permitted only upon receipt of a certification by the plan sponsor that the plan documents have been amended and the plan sponsor agrees to certain restrictions on the use of protected health information; and provide for adequate firewalls to assure unauthorized personnel do not have access to individually identifiable health information.

Some plan sponsors may need information, not to administer the group health plan, but to amend, modify, or terminate the health plan. ERISA case law describes such activities as settlor functions. For example a plan sponsor may want to change its contract from a preferred provider organization to a health maintenance organization (HMO). In order to obtain premium information, the health plan sponsor may need to provide the HMO with aggregate claims information. Under the rule, the health plan sponsor can obtain summary information with certain identifiers removed, in order to provide it to the HMO and receive a premium rate.

The Department assumes that most health plan sponsors who are small employers (those with 50 or fewer employees) will elect not to receive individually identifiable health information because they will have little, if any, need for such data. Any needs that sponsors of small group health plans may have for information can be accomplished by receiving the information in summary form from their health insurance issuers.

3. The Burden on a Typical Small Business

The Department expects small entities to 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 could be a larger burden to small entities as a proportion of total revenue. Due to these concerns, we have relied on the principle of scalability throughout the rule, and have based our cost estimates on the expectation that small entities will develop less expensive and less complex privacy measures that comply with the rule than large entities.

In many cases, we have specifically considered the impact that rule may have on solo practitioners or rural health care providers. If a health care provider only maintains paper records and does not engage in any electronic transactions, the regulation would not apply to such provider. We assume that those providers will be small health care providers. For small health care providers that are covered health care providers, we expect that they will not be required to change their business practices dramatically, because we based many of the standards, implementation specifications, and requirements on current practice and we have taken a flexible approach to allow scalability based on a covered entity's activities and size. In developing policies and procedures to comply with the proposed regulation, scalability allows entities to consider their basic functions and the ways in which protected health information is used or disclosed. 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 within the requirements of the rule.

Cost Assumptions

To determine the cost burden to small businesses of complying with the final rule, we used as a starting point the overall cost of the regulation determined

in the regulatory impact analysis (RIA). Then we adopted a methodology that apportions the costs found in the RIA to small business by using Census Bureau's Statistics of U.S. Businesses. This Census Bureau survey contains data on the number and proportion of establishments, by Standard Industrial Classification Code (SIC code), that have revenues of less than $5 million, which meets the Small Business Administration's definition of a small business in the health care sector. This data permitted us to calculate the proportion of the cost of each requirement in the rule that is attributable to small businesses. This methodology used for the regulatory flexibility analysis (RFA) section is therefore based on the methodology used in the (RIA), which was discussed earlier.

The businesses accounted for in the SIC codes contain three groups of covered entities: non-hospital health care providers, hospitals, and health plans. Non-hospital health care providers include: drug stores, offices and clinics of doctors, dentists, osteopaths, and other health practitioners, nursing and personal care facilities, medical and dental laboratories, home health care services, miscellaneous health and allied services, and medical equipment rental and leasing establishments. Health plans include accident and health insurance and medical service plans.

Data Adjustments

Several adjustments were made to the SIC code data to more accurately determine the cost to small and non-profit businesses. For health plans (SIC code 6320), we adjusted the SIC data to include self-insured, self-administered health plans because these health plans are not included in any SIC code, though they are covered entities under the rule. Similarly, we have added third-party administrators (TPAs) into this SIC. Although they are not covered entities, TPAs are likely to be business associates of covered entities. For purposes of the regulatory analyses, we have assumed that TPAs would bear many of the same costs of the health plans to assure compliance for the covered entity. To make this adjustment, we assumed the self-insured/self administered health plans and TPAs have the average revenue of the health plans contained in the SIC code, and then added those assumed revenues to the SIC code and to the total of all health care expenditures. Moreover, we needed to account for the cost to non-profit institutions that might receive more than $5 million in revenue, because all non-profit institutions are small businesses regardless of revenue. To make this adjustment for hospitals, nursing homes, and home health agencies, we used data on the number of non-profit institutions from industry sources and from data reported to HCFA. With this data, we assumed the current count of establishments in the SIC codes includes these non-profit entities and that non-profits have the same distribution of revenues as all establishments reported in the applicable SIC codes. The proportions discussed below, which determine the cost for small business, therefore include these non-profit establishments in SIC codes 8030, 8060, and 8080.

The SIC code tables provided in this RFA do not include several categories of businesses that are included in the total cost to small businesses. Claims clearinghouses are not included in the table because claims clearinghouses report their revenues under the SIC 7374 ''Computer Processing and Data Preparation,'' and the vast majority of businesses in this SIC code are involved in non-medical claims data processing. In addition, claims processing is often just one business-line of companies that may be involved in multiple forms of data processing, and therefore, even if the claims processing line of the business generates less than $5 million in revenue, the company in total may exceed the SBA definition for a small business (the total firm revenue, not each line of business, is the standard for inclusion). Similarly, fully-insured ERISA health plans sponsored by employers are not identified as a separate category in the SIC code tables because employers in virtually all SIC codes may sponsor fully-insured health plans. We have identified the cost for small fully-insured ERISA health plans by using the Department of Labor definition of a small ERISA plan, which is a plan with fewer than 100 insured participants. Using this definition, the initial cost for small fully-insured ERISA health plans is $7.1 million. Finally, Institutional Review Boards (IRBs) will not appear in a separate SIC code because IRBs are not ''businesses''; rather, they are committees of researchers who work for institutions where medical research is conducted, such as universities or teaching hospitals. IRB members usually serve as a professional courtesy or as part of their employment duties and are not paid separately for their IRB duties. Although IRBs are not ''businesses'' that generate revenues, we have treated them as small business for illustrative purposes in this RFA to demonstrate the additional opportunity costs that will be faced by those researchers who sit on IRBs. Therefore, assuming IRBs are small businesses, the initial costs are $.089 million and ongoing costs are approximately $84.2 million over 9 years.

The Cost Model Methodology

The RIA model employs two basic methodologies to determine the costs to small businesses that are covered entities. As stated above, the RFA determines the cost to small businesses by apportioning the total costs in the RIA using SIC code data. In places where the cost of a given provision of the final rule is a function of the number of covered entities, we determined the proportion of entities in each SIC code that have less than $5 million in revenues (see Table A). We then multiplied this proportion by the per-entity cost estimate of a given provision as determined in the RIA. For example, the cost of the privacy official provision is based on the fact that each covered entity will need to have a privacy official. Therefore, we multiplied the total cost of the privacy official, as determined in the RIA, by the proportion of small businesses in each SIC code to determine the small business cost. Using hospitals for illustrative purposes, because small and non-profit hospitals account for 50 percent of all hospitals, our methodology assigned 50 percent of the cost to small hospitals.

We used a second, though similar, method when the cost of a given provision in the RIA did not depend on the number of covered entities. For example, the requirement to provide notice of the privacy policy is a direct function of the number of patients in the health care system because the actual number of notices distributed depends on how many patients are seen. Therefore, for provisions like the notice requirement, we used SIC code revenue data in a two-step process. First, we apportioned the cost of each provision among sectors of the health care industry by SIC code. For example, because hospital revenue accounts for 27 percent of all health care revenue, we multiplied the total cost of each such provision by 27 percent to determine the cost for the hospital sector in total. Then to determine the cost for small hospitals specifically, we calculated the proportion by the overall cost. For example, 45.1 percent of all hospital revenue is generated by small hospital, therefore, the cost to small hospitals was assumed to account for 45.1 percent of all hospital costs. Estimates, by nature

are inexact. However, we feel this is a reasonable way to determine the small business costs attributable to this regulation given the limited data from which to work.

Total Costs and Costs Per Establishment for Small Business

Based on the methodology described above, the total cost of complying with the final rule in the initial year of 2003 is $1.9 billion. The ongoing costs to small business from 2004 to 2012 is $9.3 billion. Table C presents the initial and ongoing costs to small business by each SIC code. According to this table, small doctors offices, small dentists offices and small hospitals will face the highest cost of complying with the final rule. However, much of the reason for the higher costs faced by these three groups of small health care providers is explained by the fact that there are a significant number of health care providers in these categories.

BILLING CODE 4150–04–P

Table C.--Annual Cost to Small Business of Implementing Provisions of the Proposed Privacy Regulation[1]

SIC	Industry	Initial Cost (Year 1)[1]	Ongoing Cost (Year 2-10)	Total Costs
5910	Drug Stores & Proprietary Stores	$153,976,159	$780,573,862	$934,550,021
6320	Accident & Health Insurance & Medical Service Plans[2]	$41,348,527	$169,540,638	$210,889,164
7353	Medical Equipment Rental & Leasing	$7,171,728	$36,356,688	$43,528,416
8010	Offices & Clinics of Doctors of Medicine	$633,033,192	$3,209,127,747	$3,842,160,938
8120	Offices & Clinics of Dentists	$283,774,344	$1,438,578,786	$1,722,353,130
8030	Offices & Clinics of Doctors of Osteopathy	$24,278,673	$123,079,430	$147,358,103
8040	Offices & Clinics of Other Health Practitioners	$139,251,750	$705,929,263	$845,181,013
8050	Nursing & Personal Care Facilities	$147,143,775	$745,937,461	$893,081,236
8060	Hospitals	$355,459,094	$1,199,498,063	$1,554,957,157
8070	Medical & Dental Laboratories	$41,242,809	$209,078,203	$250,321,012
8080	Home Health Care Services	$72,632,601	$368,207,067	$440,839,668
8090	Misc Health & And Allied Services	$40,938,582	$207,535,943	$248,474,525
n/a	Fully Insured/ ERISA	$7,137,028	$0	$7,137,028
n/a	IRBs	$88,813	$84,162,446	$84,251,259
n/a	Total Cost For Small Business	$1,947,477,073	$9,277,605,598	$11,225,082,671

[1] Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997. Entities that have less than $5,000,000 in annual revenue are considered small businesses here, as are non-profit entities (regardless of revenue). We have non-profit data for the following SICs: 8050, 8080, and 8060 and have included the number of non-profits in each category into the table.

[2]The initial costs include all costs in the first year, including costs that recur in subsequent years.

[3] We have included self-insured/self-administered health plans and third party administrators in the total number of health plans, even though neither has individual SIC codes because we have the ability to impute revenues to them.

On a per-establishment basis, Table D demonstrates that the average cost for small business of complying with the proposed rule in the first year is $4,188 per-establishment. The ongoing costs of privacy compliance are approximately $2,217 each year thereafter. We estimate that the average cost of compliance in the first year for each small non-hospital health care provider is approximately 0.6 percent of per-establishment revenues. In subsequent years, per-establishment costs about 0.3 percent of per-establishment revenues. For small hospitals and health plans, the per-establishment cost of compliance in the first year is 0.2 percent and 6.3 percent of per-establishment revenues respectively. For subsequent years, the cost is only 0.1 percent and 2.9 percent of pre-establishment revenues respectively. These costs may be offset in many firms by the savings realized through requirements of the Transactions Rule.

Table D.--Average Annual per Establishment Privacy Costs[1]

SIC	Industry	Year 1 Privacy Costs Per Establishment	Average Year 2-10 Privacy Costs per Establishment
5910	Drug Stores & Proprietary Stores	$6,436	$3,625
6320	Accident & Health Insurance & Medical Service Plans[2]	$62,162	$28,320
7353	Medical Equipment Rental & Leasing	$3,906	$2,200
8010	Offices & Clinics of Doctors of Medicine	$3,703	$2,086
8120	Offices & Clinics of Dentists	$2,492	$1,404
8030	Offices & Clinics of Doctors of Osteopathy	$2,743	$1,545
8040	Offices & Clinics of Other Health Practioners	$1,608	$906
8050	Nursing & Personal Care Facilities	$8,301	$4,676
8060	Hospitals	$101,999	$38,244
8070	Medical & Dental Laboratories	$3,169	$1,785
8080	Home Health Care Services	$5,656	$3,186
8090	Misc Health & And Allied Services	$3,649	$2,055
n/a	Fully Insured/ ERISA[3]	N/A	N/A
n/a	IRB[3]	N/A	N/A
n/a	Average for All Small Business	$4,188	$2,217

[1] Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997. Entities that have less than $5,000,000 in annual revenue are considered small businesses here, as are non-profit entities (regardless of revenue). We have non-profit data for the following SICs: 8050, 8080, and 8060 and have included the number of non-profits in each category into the table.

[2] We have included self-insured/self-administered health plans and third party administrators in the total number of health plans, even though neither has individual SIC codes because we have the ability to impute revenues to them.

[2]We have not included the number of fully insured ERISA health plans or institutional review boards (IRB) in the total number of health care entities or the number of entities that meet SMA standards for small entities, since these are not separate businesses with SIC codes and we do not have sufficient data to impute revenues to them.

Table E shows the cost to each SIC code of the major cost items of the final rule. Listed are the top-five most costly provisions of the rule (to small business) and then the cost of all other remaining provisions. The costs of the most expensive five provisions represent 90 percent of the cost of the ongoing costs to small business, while the remaining provisions only represent 7 percent.

Table E.—Average Annual Ongoing Cost to Small Business of Implementing Provisions of the Privacy Regulation, After the First Year [1]

Industry	Average Annual Ongoing Cost for Privacy Official, per Industry Sector	Average Annual Ongoing Cost for Minimum Necessary, per Industry Sector	Average Annual Ongoing Cost for Disclosure Tracking, per Industry Sector	Average Annual Ongoing Cost for De-Identification, per Industry Sector	Average Annual Ongoing Cost for Training, per Industry Sector	Average Annual Ongoing Cost for All Other Provisions, per Industry Sector
Drug Stores & Proprietary Stores	$37,997,168	$30,008,085	$3,597,262	$3,751,011	$4,083,677	$7,293,227
Accident & Health Insurance & Medical Service plans (including Self Insured/ Self Administered Health plans, & TPAs)[2]	$5,920,267	$5,395,070	$985,072	$3,614,697	$59,086	$2,863,657
Medical Equipment Rental & Leasing	$1,769,789	$1,397,683	$167,549	$174,710	$190,205	$339,696
Offices & clinics of Doctors of Medicine	$156,215,538	$123,370,486	$14,789,213	$15,421,311	$16,788,984	$29,984,217

Offices & clinics of Doctors of Dentists	$70,027,863	$55,304,176	$6,629,667	$6,913,022	$7,526,119	$13,441,241
Offices & clinics of Doctors of Osteopathy	$5,991,323	$4,731,619	$567,210	$591,452	$643,907	$1,149,982
Offices & clinics of Other Health Practitioners	$34,363,581	$27,138,476	$3,253,264	$3,392,310	$3,693,164	$6,595,791
Nursing & Personal care Facilities	$36,311,120	$28,676,536	$3,437,641	$3,584,567	$3,902,472	$6,969,604
Hospitals	$25,475,393	$56,613,285	$19,558,912	$14,153,321	$309,555	$17,167,095
Medical & Dental Laboratories	$10,177,614	$8,037,723	$963,534	$1,004,715	$1,093,821	$1,953,505
Home Health care Services	$17,923,769	$14,155,212	$1,696,876	$1,769,402	$1,926,325	$3,440,312
Misc Health & Allied Health Services	$10,102,539	$7,978,433	$956,426	$997,304	$1,085,752	$1,939,095
Fully Insured/ERISA	N/A	N/A	N/A	N/A	N/A	$9,351,383
IRB	N/A	N/A	N/A	N/A	N/A	$0
Total	$412,275,964	$362,806,784	$56,602,625	$55,367,822	$41,303,067	$102,488,804

[1] Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997. Entities that have less than $5,000,000 in annual revenue are considered small businesses here, as are

[2] We have included self-insured, self-administered health plans and third party administrators in the total number of health plans, even though neither has individual SIC codes because we have the ability to impute revenues to them.

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 rule qualifies as a significant rule under the statute. The Department has carried out the cost-benefit analysis in sections D and E of this document, which includes a discussion of unfunded costs to state and local governments resulting from this regulation. In developing this regulation, the Department adopted the least burdensome alternatives, consistent with achieving the rule's goals.

A. Future Costs

The Department estimates some of the future costs of the rule in Section E of the Preliminary Regulatory Impact Analysis of this document. The estimates made include costs for the ten years after the effective date. As discussed in section E, state and local government costs will be in the order of $460 million in 2003 and $2.4 billion over ten years. Estimates for later years are not practical. The changes in technology are likely to alter the nature of medical record-keeping, and the uses of medical data are likely to vary dramatically over this period. Therefore, any estimates for years beyond 2012 are not feasible.

B. Particular Regions, Communities, or Industrial Sectors

The 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. However, as discussed in the administrative implication regulation, the Transactions Rule is estimated to save the health care industry nearly $30 billion over essentially the same time period. This more than offsets the costs of the Privacy Rule; indeed, as discussed above, the establishment of consistent, national standards for the protection of medical information is essential to fully realize the savings from electronic transactions standards and other advances that may be realized through ''e-health'' over the next decade. Without strong privacy rules, patients and providers may be very reluctant to fully participate in electronic and e-health opportunities.

C. National Productivity and Economic Growth

The 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, the Department anticipates that, because the benefits of privacy are large, both productivity and economic growth would be higher than in the absence of the final rule. In section I.A. of this document, the Department discusses its expectation that this rule will 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 the delivery of health care services will be redirected by rule. The 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 health care profession could also temporarily change but be balanced by an increased need for those who can assist entities with complying with this 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 rule (*e.g.* worker training, and management consultants).

E. Exports

Because the rule does not mandate any changes in products, current export products will not be required to change in any way.

The Department consulted with state and local governments, and Tribal governments. See sections X and XI, below.

VII. Environmental Impact

The Department has determined under 21 CFR 25.30(k) that this action is of a type of 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 30-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 V (Final 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 assumptions as they relate to the PRA requirements summarized in this section.

Section 160.204—Process for Requesting Exception Determinations

Section 160.204 would require persons requesting to except a provision of state law from preemption under § 160.203(a) to 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. The burden associated with these requirements is the time and effort necessary for a state to prepare and submit the written request for an exception determination to the Secretary for approval. On an annual basis it is estimated that it will take 40 states 16 hours each to prepare and submit a request. The total annual burden associated with this requirement is 640 hours. The Department solicits public comment on the number of requests and hours for others likely to submit requests.

Section 160.306—Complaints to the Secretary

A person who believes that a covered entity is not complying with the applicable requirements of part 160 or the applicable standards, requirements,

and implementation specifications of Subpart E of part 164 of this subchapter may file a complaint with the Secretary. This requirement is exempt from the PRA as stipulated under 5 CFR 1320.4(a)(2), an audit/administrative action exemption.

Section 160.310—Responsibilities of Covered Entities

A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements of part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164. Refer to § 164.530 for discussion.

Section 164.502—Uses and Disclosures of Protected Health Information: General Rules

A covered entity is permitted to disclose protected health information to an individual, and is required to provide and individual with access to protected health information, in accordance with the requirements set forth under § 164.524. Refer to § 164.524 for discussion.

Section 164.504—Uses and Disclosures—Organizational 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, § 164.504 requires a covered entity to maintain documentation demonstrating that it meets the requirements set forth in this section and to demonstrate that it has obtained satisfactory assurance from business associates that meet the requirements of this part with each of its business associates. The burden is 5 minutes per entity times an annual average of 764,799 entities for a total burden of 63,733 burden hours.

Section 164.506—Consent for Treatment, Payment, and Health Care Operations

Except in certain circumstances, a covered health care provider that has a direct treatment relationship must obtain an individual's consent for use or disclosure of protected health information for treatment, payment, or health care operations. While this requirement is subject to the PRA, we believe that the burden associated with this requirement is exempt from the PRA as stipulated under 5 CFR 1320.3(b)(2).

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

Under this section, a covered entity will need to obtain a written authorization from an individual, before it uses or discloses protected health information of the individual if the use or disclosure is not otherwise permitted or required under the rule without authorization. The burden associated with these requirements is the time and effort necessary for a covered entity to obtain written authorization prior to the disclosure of individually identifiable health information. On an annual basis, we estimate that it will take 764,799 entities, an annual average burden per entity of one hour for a total annual burden of 764,799 burden hours.

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

Section 164.510 allows, but does not require, covered entities to use or disclose protected health information: (1) for health care institutions, directories; and (2) to family members, close friends, or other persons assisting in an individual's care, as well as government agencies and disaster relief organizations conducting disaster relief activities. This section of the rule addresses situations in which the interaction between the covered entity and the individual is relatively informal, and agreements may be made orally, without written authorizations for use or disclosure. In general, to disclose protected health information for these purposes, covered entities must inform individuals in advance and must provide a meaningful opportunity for the individual to prevent or restrict the disclosure. In certain circumstances, such as in an emergency, when this informal discussion cannot practicably occur, covered entities can make decisions about disclosure or use, in accordance with the requirements of this section based on their professional judgment of what is in the patient's best interest. While these provisions are subject to the PRA, we believe that the burden associated with this requirement is exempt from the PRA as stipulated under 5 CFR 1320.3(b)(2).

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

Section 164.1512 includes provisions that allow, but that do not require, covered entities to disclose protected health information without individual authorization for a variety of purposes which represent important national priorities. Pursuant to § 164.512, covered entities may disclose protected health information for specified purposes as follows: as required by law; for public health activities; to public officials regarding victims of abuse, neglect, or domestic violence; for health oversight; for judicial and administrative proceedings; for law enforcement; for specified purposes regarding decedents; for organ donation and transplantation; for research; to avert an imminent threat to health or safety; for specialized government functions (such as for intelligence and national security activities); and to comply with workers' compensation laws. While these provisions are subject to the PRA, we believe that the burden associated with this requirement is exempt from the PRA as stipulated under 5 CFR 1320.3(b)(2).

For research, if a covered entity wants to use or disclose protected health information without individual authorization, it must obtain documentation that a waiver, in whole or in part, of the individual authorization required by § 164.508 for use or disclosure of protected health information has been approved by either an Institutional Review Board (IRB), 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 a privacy board. The burden associated with these requirements is the time and effort necessary for a covered entity to maintain documentation demonstrating that they have obtained IRB or privacy board approval, which meet the requirements of this section. On an annual basis it is estimated that these requirements will affect 113,524 IRB reviews. We further estimate that it will take an average of 5 minutes per review to meet these requirements on an annual basis. Therefore, the total estimated annual burden associated with this requirement is 9,460 hours.

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

Prior to any disclosure permitted by this subpart, a covered entity must verify the identity and authority of persons requesting protected health information, if the identity or authority of such person is not known to the

covered entity, and obtain any documentation, statements, or representations from the person requesting the protected health information that is required as a condition of the disclosure. In addition, a covered entity must retain any signed consent pursuant to § 164.506 and any signed authorization pursuant to § 164.508 for documentation purposes as required by § 164.530(j). This requirement is exempt from the PRA as stipulated under 5 CFR 1320.4(a)(1) and (1)(2).

Section 164.520—Notice of Privacy Practices for Protected Health Information

Except in certain circumstances set forth in this section, individuals have a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information. To comply with this requirement a covered entity must provide a notice, written in plain language, that includes the elements set forth in this section. For health plans, there will be an average of 160.2 million notices each year. We assume that the most efficient means of distribution for health plans will be to send them out annually as part of the materials they send to current and potential enrollees, even though it is not required by the regulation. The number of notices per health plan per year would be about 10,570. We further estimate that it will require each health plan, on average, only 10 seconds to disseminate each notice. The total annual burden associated with this requirement is calculated to be 267,000 hours. Health care providers with direct treatment relationships would provide a copy of the notice to an individual at the time of first service delivery to the individual, make the notice available at the service delivery site for individuals to request and take with them, whenever the content of the notice is revised, make the notice available upon request and post the notice, if required by this section, and 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. The annual number of notices disseminated by all providers is 613 million. We further estimate that it will require each health provider, on average, 10 seconds to disseminate each notice. This estimate is based upon the assumption that the required notice will be incorporated into and disseminated with other patient materials. The total annual burden associated with this requirement is calculated to be 1 million hours.

In addition, a covered entity must document compliance with the notice requirements by retaining copies of the notices issued by the covered entity. Refer to § 164.530 for discussion.

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

Given that the burden associated with the following information collection requirements will differ significantly, by the type and size of health plan or health care provider, we are explicitly soliciting comment on the burden associated with the following requirements; as outlined and required by this section, covered entities must provide individuals with the opportunity to request restrictions related to the uses or disclosures of protected health information for treatment, payment, or health care operations. In addition, covered entities must accommodate requests for confidential communications in certain situations.

Section 164.524—Access of Individuals to Protected Health Information

As set forth in this section, covered entities must provide individuals with access to inspect and obtain a copy of protected health information about them in designated record sets, for so long as the protected health information is maintained in the designated record sets. This includes such information in a business associate's designated record set that is not a duplicate of the information held by the health care provider or health plan for so long as the information is maintained. Where the request is denied in whole or in part, the covered entity must 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 § 164.530 or to the Secretary pursuant to the procedures established in § 160.306 of this subpart. In certain cases, the covered entity must provide the individual the opportunity to have another health care professional review the denial. Pursuant to public comment, we estimate that each disclosure will contain 31 pages and that 150,000 disclosures will be made on an annual basis at three minutes per disclosure for a total burden of 7,500 hours. Refer to section V.E. for detailed discussion related to the costs associated with meeting these requirements.

Section 164.526—Amendment of Protected Health Information

Given that burden associated with the following information collection requirements will differ significantly, by the type and size of health plan or health care provider, we are explicitly soliciting comment on the burden associated with the following requirements: Individuals have the right to request amendment of protected health information about them in designated record sets created by a covered entity. Where the request is denied, a covered entity must provide the individual with a written statement of the basis for the denial and an explanation of how the individual may pursue the matter, including how to file a complaint with the Secretary pursuant to § 160.306 of this subpart. As appropriate, a covered entity must identify the protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

Section 164.528—Accounting for Disclosures of Protected Health Information

Based upon public comment it is assumed that it will take 5 minutes per request times 1,081,000 requests for an annual burden of 90,083 hours. An individual may request that a covered entity provide an accounting for disclosure for a period of time less than six years from the date of the individual's request, as outlined in this section.

Section 164.530—Administrative Requirements

A covered entity must maintain such policies and procedures in written or electronic form where policies or procedures with respect to protected health information are required by this subpart. Where a communication is required by this subpart to be in writing, a covered entity must maintain such writing, or an electronic copy, as documentation; and where an action or activity is required by this subpart to be documented, it must maintain a written or electronic record of such action or activity. While these requirements are subject to the PRA, we believe the burden associated with these requirements is exempt from the PRA as stipulated under 5 CFR 1320.3(b)(2).

We have submitted a copy of this rule to OMB for its review of the information collection requirements in §§ 160.204, 160.306, 160.310, 164.502, 164.504, 164.506, 164.508, 164.510, 164.512, 164.514, 164.520, 164.522, 164.524, 164.526, 164.528, and Sec. 164.530. 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, Division of HCFA Enterprise Standards, Room N2–14–26, 7500 Security Boulevard, Baltimore, MD 21244–1850. ATTN: John Burke and to the 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 13132: Federalism

The Department has examined the effects of provisions in the final privacy regulation on the relationship between the federal government and the states, as required by Executive Order 13132 on ''Federalism.'' Our conclusion is that the final rule does have federalism implications because the rule has substantial direct effects on states, on the relationship between the national government and states, and on the distribution of power and responsibilities among the various levels of government. The federalism implications of the rule, however, flow from, and are consistent with the underlying statute. The statute allows us to preempt state or local rules that provide less stringent privacy protection requirements than federal law is consistent with this Executive Order. Overall, the final 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 statue dictates the relationship between state law and this final 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 of state law relating to the privacy of individually identifiable health information that are also ''more stringent'' than the federal regulatory requirements or implementation specifications will continue to be enforceable.

Section 3(b) of Executive Order 13132 recognizes that national action limiting the policymaking discretion of states will be imposed ''* * * only where there is constitutional and statutory authority for the action and the national activity is appropriate in light of the presence of a problem of national significance.'' 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 13132 requires the federal government defer to the states to establish standards where possible. HIPAA requires the Department to establish standards, and we have done so accordingly. This approach is a key component of the final Privacy Rule, and it adheres to section 4(a) of Executive Order 13132, 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 ''the exercise of state authority is directly conflicts with the exercise of federal authority under federal statute * * *.'' 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 final rule would establish national minimum standards with respect to the collection, maintenance, access, use, and disclosure of individually 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 previous Executive Order (E.O. 13132), states and local governments were given, through the notice of proposed rule making, an opportunity to participate in the proceedings to preempt state and local laws (section 4(e)). The Secretary also provided a review of preemption issues upon requests from states. In addition, anticipating the promulgation of the Executive Order, appropriate officials and organizations were consulted before this proposed action is implemented (Section 3(a) of Executive Order 13132).

The same section also includes some qualitative discussion of costs that would occur beyond that time period. Most of the costs of proposed rule, however, would occur in the years immediately after the publication of a final rule. Future costs beyond the ten year period will continue but will not be as great as the initial compliance costs.

Finally, we have considered the cost burden that this proposed rule would impose on state and local health care programs, such as Medicaid, county hospitals, and other state health benefits programs. As discussed in Section E of the Regulatory Impact Analysis of this document, we estimate state and local government costs will be in the order of $460 million in 2003 and $2.4 billion over ten years.

The agency concludes that the policy in this final document has been assessed in light of the principles, criteria, and requirements in Executive Order 13132; 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 final regulation would preempt

all state privacy laws. As explained in this section, the regulation would only preempt 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

45 CFR Part 160

Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Medicaid, Medical research, Medicare, Privacy, Reporting and record keeping requirements.

45 CFR Part 164

Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Medicaid, Medical research, Medicare, Privacy, Reporting and record keeping requirements.

Note: to reader: This final rule is one of several proposed and final rules that are being published to implement the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996. 45 CFR subchapter C consisting of Parts 160 and 162 was added at 65 FR 50365, Aug. 17, 2000. Part 160 consists of general provisions, Part 162 consists of the various administrative simplification regulations relating to transactions and identifiers, and new Part 164 consists of the regulations implementing the security and privacy requirements of the legislation.

Dated: December 19, 2000.

Donna Shalala,

Secretary,

For the reasons set forth in the preamble, 45 CFR Subtitle A, Subchapter C, is amended as follows:

1. Part 160 is revised to read as follows:

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

Subpart A—General Provisions

Subpart B—Preemption of State Law

Subpart C—Compliance and Enforcement

Authority: Sec. 1171 through 1179 of the Social Security Act, (42 U.S.C. 1320d–1329d–8) as added by sec. 262 of Pub. L. 104–191, 110 Stat. 2021–2031 and sec. 264 of Pub. L. 104–191 (42 U.S.C. 1320d–2(note)).

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 (the Act), as added by section 262 of Public Law 104–191, and section 264 of Public Law 104–191.

§ 160.102 Applicability.

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) To the extent required under section 201(a)(5) of the Health Insurance Portability Act of 1996, (Pub. L. 104–191), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

§ 160.103 Definitions.

Except as otherwise provided, the following definitions apply to this subchapter:

Act means the Social Security Act.

ANSI stands for the American National Standards Institute.

Business associate: (1) Except as provided in paragraph (2) of this definition, *business associate* means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service,

become a business associate of other covered entities participating in such organized health care arrangement.

(3) A covered entity may be a business associate of another covered entity.

Compliance date means the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

Covered entity means:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Group health plan (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 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 (PHS 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, reimbursement, or otherwise, that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

(2) Is administered by an entity other than the employer that established and maintains the plan.

HCFA stands for Health Care Financing Administration within the Department of Health and Human Services.

HHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and ''value-added'' networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care 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 insurance issuer (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg–91(b)(2) and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg–91(b)(3) and used in the definition of *health plan* in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

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

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, *et seq.*

(vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.

(viii) 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.

(ix) The health care program for active military personnel under title 10 of the United States Code.

(x) The veterans health care program under 38 U.S.C. chapter 17.

(xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)).

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

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, *et seq.*

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, *et seq.*

(xv) The Medicare+Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w–21 through 1395w–28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(2) *Health plan* excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg–91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)–(xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(1) The direct provision of health care to persons; or

(2) The making of grants to fund the direct provision of health care to persons.

Implementation specification means specific requirements or instructions for implementing a standard.

Modify or *modification* refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS 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 rule, condition, or requirement:

(1) Describing the following information for products, systems, services or practices:

(i) Classification of components.

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

(2) With respect to the privacy of individually identifiable health information.

Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claim 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.

(11) Other transactions that the Secretary may prescribe by regulation.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

§ 160.104 Modifications.

(a) Except as provided in paragraph (b) of this section, the Secretary may adopt a modification to a standard or implementation specification adopted under this subchapter no more frequently than once every 12 months.

(b) The Secretary may adopt a modification at any time during the first year after the standard or implementation specification is initially adopted, if the Secretary determines that the modification is necessary to permit compliance with the standard or implementation specification.

(c) The Secretary will establish the compliance date for any standard or implementation specification modified under this section.

(1) The compliance date for a modification is no earlier than 180 days after the effective date of the final rule in which the Secretary adopts the modification.

(2) The Secretary may consider the extent of the modification and the time needed to comply with the modification in determining the compliance date for the modification.

(3) The Secretary may extend the compliance date for small health plans, as the Secretary determines is appropriate.

Subpart B—Preemption of State Law

§ 160.201 Applicability.

The provisions of this subpart implement section 1178 of the Act, as added by section 262 of Public Law 104–191.

§ 160.202 Definitions.

For purposes 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 covered entity 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 State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

(i) Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or

(ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual who is the subject of the individually identifiable health information of access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable; provided that, nothing in this subchapter may be construed to preempt any State law to the extent that it authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian, or person acting *in loco parentis* of such minor.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form or substance of an authorization or consent for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the authorization or consent, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

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 affects the privacy of health information in a direct, clear, and substantial way.

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

§ 160.203 General rule and exceptions.

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:

(a) A determination is made by the Secretary under § 160.204 that the provision of State law:

(1) Is necessary:

(i) To prevent fraud and abuse related to the provision of or payment for health care;

(ii) To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;

(iii) For State reporting on health care delivery or costs; or

(iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

(2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

(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, including State procedures established under such law, as applicable, provides 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, or the licensure or certification of facilities or individuals.

§ 160.204 Process for requesting exception determinations.

(a) A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:

(1) The State law for which the exception is requested;

(2) The particular standard, requirement, or implementation specification for which the exception is requested;

(3) 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;

(4) How health care providers, health plans, and other entities would be affected by the exception;

(5) 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

(6) Any other information the Secretary may request in order to make the determination.

(b) Requests for exception under this section must be submitted to the Secretary at an address that 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.

(c) The Secretary's determination under this section 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.

§ 160.205 Duration of effectiveness of exception determinations.

An exception granted under this subpart remains in effect until:

(a) Either the State law or the federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or

(b) The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

Subpart C—Compliance and Enforcement

§ 160.300 Applicability.

This subpart applies to actions by the Secretary, covered entities, and others with respect to ascertaining the compliance by covered entities with and the enforcement of the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.302 Definitions.

As used in this subpart, terms defined in § 164.501 of this subchapter have the same meanings given to them in that section.

§ 160.304 Principles for achieving compliance.

(a) *Cooperation.* The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(b) *Assistance.* The Secretary may provide technical assistance to covered entities to help them comply voluntarily with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.306 Complaints to the Secretary.

(a) *Right to file a complaint.* A person who believes a covered entity is not complying with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter may file a complaint with the Secretary.

(b) *Requirements for filing complaints.* Complaints under this section must meet the following requirements:

(1) A complaint must be filed in writing, either on paper or electronically.

(2) A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.

(4) The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the **Federal Register**.

(c) *Investigation.* The Secretary may investigate complaints filed under this section. Such investigation may include a review of the pertinent policies, procedures, or practices of the covered entity and of the circumstances regarding any alleged acts or omissions concerning compliance.

§ 160.308 Compliance reviews.

The Secretary may conduct compliance reviews to determine whether covered entities are complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.310 Responsibilities of covered entities.

(a) *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 applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(b) *Cooperate with complaint investigations and compliance reviews.* A covered entity must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of a covered entity to determine whether it is complying with the applicable requirements of this part 160 and the standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(c) *Permit access to information.* (1) A covered entity must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity must permit access by the Secretary at any time and without notice.

(2) If 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.

(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter, or if otherwise required by law.

§ 160.312 Secretarial action regarding complaints and compliance reviews.

(a) *Resolution where noncompliance is indicated.* (1) If an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates a failure to comply, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant, in writing and attempt to resolve the matter by informal means whenever possible.

(2) If the Secretary finds the covered entity is not in compliance and determines that the matter cannot be resolved by informal means, the Secretary may issue to the covered entity and, if the matter arose from a complaint, to the complainant written findings documenting the non-compliance.

(b) *Resolution when no violation is found.* If, after an investigation or compliance review, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant in writing.

2. A new Part 164 is added to read as follows:

PART 164—SECURITY AND PRIVACY

Subpart A—General Provisions

Sec.

Subparts B–D—[Reserved]

Subpart E—Privacy of Individually Identifiable Health Information

Authority: 42 U.S.C. 1320d–2 and 1320d–4, sec. 264 of Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320(d–2(note)).

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.

§ 164.106 Relationship to other parts.

In complying with the requirements of this part, covered entities are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

Subpart B–D—[Reserved]

Subpart E—Privacy of Individually Identifiable Health Information

§ 164.500 Applicability.

(a) Except as otherwise provided herein, the standards, requirements, and

implementation specifications of this subpart apply to covered entities with respect to protected health information.

(b) Health care clearinghouses must comply with the standards, requirements, and implementation specifications as follows:

(1) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, the clearinghouse must comply with:

(i) Section 164.500 relating to applicability;

(ii) Section 164.501 relating to definitions;

(iii) Section 164.502 relating to uses and disclosures of protected health information, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(iv) Section 164.504 relating to the organizational requirements for covered entities, including the designation of health care components of a covered entity;

(v) Section 164.512 relating to uses and disclosures for which consent, individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(vi) Section 164.532 relating to transition requirements; and

(vii) Section 164.534 relating to compliance dates for initial implementation of the privacy standards.

(2) When a health care clearinghouse creates or receives protected health information other than as a business associate of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of this subpart.

(c) The standards, requirements, and implementation specifications of this subpart do not apply to the Department of Defense or to any other federal agency, or non-governmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.

§ 164.501 Definitions.

As used in this subpart, the following terms have the following meanings:

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons* held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Designated record set means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

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 any of the following activities of the covered entity to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity; and

(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in § 164.514(e)(2).

Health oversight agency 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, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Indirect treatment relationship means a relationship between an individual and a health care provider in which:

(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and

(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Individual means the person who is the subject of protected health information.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by 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) That identifies the individual; or

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

Inmate means a person incarcerated in or otherwise confined to a correctional institution.

Law enforcement official means an officer or employee of any 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:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Marketing means to make a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service.

(1) *Marketing* does not include communications that meet the requirements of paragraph (2) of this definition and that are made by a covered entity:

(i) For the purpose of describing the entities participating in a health care provider network or health plan network, or for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits; or

(ii) That are tailored to the circumstances of a particular individual and the communications are:

(A) Made by a health care provider to an individual as part of the treatment of the individual, and for the purpose of furthering the treatment of that individual; or

(B) Made by a health care provider or health plan to an individual in the course of managing the treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care.

(2) A communication described in paragraph (1) of this definition is not included in marketing if:

(i) The communication is made orally; or

(ii) The communication is in writing and the covered entity does not receive direct or indirect remuneration from a third party for making the communication.

Organized health care arrangement means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Payment means:

(1) The activities undertaken by:

(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care 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;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan.

Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in any medium described in the definition of *electronic media* at § 162.103 of this subchapter; or

(iii) Transmitted or maintained in any other form or medium.

(2) *Protected health information* excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv).

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 and that are separated from the rest of the individual's medical record. *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.

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, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Required by law means a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

§ 164.502 Uses and disclosures of protected health information: general rules.

(a) *Standard.* A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) *Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) Pursuant to and in compliance with a consent that complies with § 164.506, to carry out treatment, payment, or health care operations;

(iii) Without consent, if consent is not required under § 164.506(a) and has not been sought under § 164.506(a)(4), to carry out treatment, payment, or health care operations, except with respect to psychotherapy notes;

(iv) Pursuant to and in compliance with a valid authorization under § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with this section, § 164.512, or § 164.514(e), (f), and (g).

(2) *Required disclosures.* A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and required by § 164.524 or § 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.

(b) *Standard: Minimum necessary.* (1) *Minimum necessary applies.* When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) *Minimum necessary does not apply.* This requirement does not apply to:

(i) Disclosures to or requests by a health care provider for treatment;

(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section, as required by paragraph (a)(2)(i) of this section, or pursuant to an authorization under § 164.508, except for authorizations requested by the covered entity under § 164.508(d), (e), or (f);

(iii) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;

(iv) Uses or disclosures that are required by law, as described by § 164.512(a); and

(v) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

(c) *Standard: Uses and disclosures of protected health information subject to an agreed upon restriction.* A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

(d) *Standard: Uses and disclosures of de-identified protected health information.*

(1) *Uses and disclosures to create de-identified information.* A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) *Uses and disclosures of de-identified information.* Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, *i.e.,* de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) *Standard: Disclosures to business associates.* (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

(ii) This standard does not apply:

(A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;

(B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or

(C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

(iii) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.504(e).

(2) *Implementation specification: documentation.* A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

(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.

(g)(1) *Standard: Personal representatives.* As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

(2) *Implementation specification: adults and emancipated minors.* If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3) *Implementation specification: unemancipated minors.* If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(i) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(ii) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis,* and the minor, a court, or another person authorized by law consents to such health care service; or

(iii) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(4) *Implementation specification: Deceased individuals.* If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(5) *Implementation specification: Abuse, neglect, endangerment situations.* Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

(i) The covered entity has a reasonable belief that:

(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

(B) Treating such person as the personal representative could endanger the individual; and

(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

(h) *Standard: Confidential communications.* A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

(i) *Standard: Uses and disclosures consistent with notice.* A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)–(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

(j) *Standard: Disclosures by whistleblowers and workforce member crime victims.*

(1) *Disclosures by whistleblowers.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) *Disclosures by workforce members who are victims of a crime.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

§ 164.504 Uses and disclosures: Organizational requirements.

(a) *Definitions.* As used in this section:

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Health care component has the following meaning:

(1) Components of a covered entity that perform covered functions are part of the health care component.

(2) Another component of the covered entity is part of the entity's health care component to the extent that:

(i) It performs, with respect to a component that performs covered functions, activities that would make such other component a business associate of the component that performs covered functions if the two components were separate legal entities; and

(ii) The activities involve the use or disclosure of protected health information that such other component creates or receives from or on behalf of the component that performs covered functions.

Hybrid entity means a single legal entity that is a covered entity and whose covered functions are not its primary functions.

Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Summary health information means information, that may be individually identifiable health information, and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

(b) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of this subpart, other than the requirements of this section, apply only to the health care component(s) of the entity, as specified in this section.

(c)(1) *Implementation specification: Application of other provisions.* In applying a provision of this subpart, other than this section, to a hybrid entity:

(i) A reference in such provision to a ''covered entity'' refers to a health care component of the covered entity;

(ii) A reference in such provision to a ''health plan,'' ''covered health care provider,'' or ''health care clearinghouse'' refers to a health care component of the covered entity if such health care component performs the functions of a health plan, covered health care provider, or health care clearinghouse, as applicable; and

(iii) A reference in such provision to ''protected health information'' refers to protected health information that is created or received by or on behalf of the health care component of the covered entity.

(2) *Implementation specifications: Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this subpart. In particular, and without limiting this requirement, such covered entity must ensure that:

(i) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which this subpart would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(ii) A component that is described by paragraph (2)(i) of the definition of *health care component* in this section does not use or disclose protected health information that is within paragraph (2)(ii) of such definition for purposes of its activities other than those described by paragraph (2)(i) of such definition in a way prohibited by this subpart; and

(iii) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by this subpart.

(3) *Implementation specifications: Responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:

(i) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility to comply with this subpart.

(ii) The covered entity has the responsibility for complying with

§ 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with this subpart, including the safeguard requirements in paragraph (c)(2) of this section.

(iii) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation as required by § 164.530(j).

(d)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this subpart.

(2) *Implementation specifications: Requirements for designation of an affiliated covered entity.* (i) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this subpart, if all of the covered entities designated are under common ownership or control.

(ii) The designation of an affiliated covered entity must be documented and the documentation maintained as required by § 164.530(j).

(3) *Implementation specifications: Safeguard requirements.* An affiliated covered entity must ensure that:

(i) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of this subpart; and

(ii) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with paragraph (g) of this section.

(e)(1) *Standard: Business associate contracts.* (i) The contract or other arrangement between the covered entity and the business associate required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (e) of this section, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(A) Terminated the contract or arrangement, if feasible; or

(B) If termination is not feasible, reported the problem to the Secretary.

(2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;

(D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(I) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) *Implementation specifications: Other arrangements.* (i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with paragraph (e) of this section by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section.

(B) The covered entity may comply with paragraph (e) of this section, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of *business associate* in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph (e), provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(3)(i) of this section, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(4) *Implementation specifications: Other requirements for contracts and other arrangements.* (i) The contract or other arrangement between the covered entity and the business associate may

permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B)(*1*) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

(*2*) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(f)(1) *Standard: Requirements for group health plans.* (i) Except as provided under paragraph (f)(1)(ii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and discloses of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of :

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan.

(2) *Implementation specifications: Requirements for plan documents.* The plan documents of the group health plan must be amended to incorporate provisions to:

(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;

(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and

(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.

(3) *Implementation specifications: Uses and disclosures.* A group health plan may:

(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;

(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;

(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and (iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

(g) *Standard: Requirements for a covered entity with multiple covered functions.*

(1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.

(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

§ 164.506 Consent for uses or disclosures to carry out treatment, payment, or health care operations.

(a) *Standard: Consent requirement.* (1) Except as provided in paragraph (a)(2) or (a)(3) of this section, a covered health care provider must obtain the individual's consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations.

(2) A covered health care provider may, without consent, use or disclose protected health information to carry out treatment, payment, or health care operations, if:

(i) The covered health care provider has an indirect treatment relationship with the individual; or

(ii) The covered health care provider created or received the protected health information in the course of providing health care to an individual who is an inmate.

(3)(i) A covered health care provider may, without prior consent, use or disclose protected health information created or received under paragraph (a)(3)(i)(A)–(C) of this section to carry out treatment, payment, or health care operations:

(A) In emergency treatment situations, if the covered health care provider attempts to obtain such consent as soon as reasonably practicable after the delivery of such treatment;

(B) If the covered health care provider is required by law to treat the individual, and the covered health care provider attempts to obtain such consent but is unable to obtain such consent; or

(C) If a covered health care provider attempts to obtain such consent from the individual but is unable to obtain such consent due to substantial barriers to communicating with the individual, and the covered health care provider determines, in the exercise of professional judgment, that the individual's consent to receive treatment is clearly inferred from the circumstances.

(ii) A covered health care provider that fails to obtain such consent in accordance with paragraph (a)(3)(i) of this section must document its attempt to obtain consent and the reason why consent was not obtained.

(4) If a covered entity is not required to obtain consent by paragraph (a)(1) of this section, it may obtain an individual's consent for the covered entity's own use or disclosure of protected health information to carry out treatment, payment, or health care operations, provided that such consent meets the requirements of this section.

(5) Except as provided in paragraph (f)(1) of this section, a consent obtained by a covered entity under this section is not effective to permit another covered entity to use or disclose protected health information.

(b) *Implementation specifications: General requirements.* (1) A covered health care provider may condition treatment on the provision by the individual of a consent under this section.

(2) A health plan may condition enrollment in the health plan on the provision by the individual of a consent under this section sought in conjunction with such enrollment.

(3) A consent under this section may not be combined in a single document with the notice required by § 164.520.

(4)(i) A consent for use or disclosure may be combined with other types of written legal permission from the individual (*e.g.,* an informed consent for treatment or a consent to assignment of benefits), if the consent under this section:

(A) Is visually and organizationally separate from such other written legal permission; and

(B) Is separately signed by the individual and dated.

(ii) A consent for use or disclosure may be combined with a research authorization under § 164.508(f).

(5) An individual may revoke a consent under this section at any time, except to the extent that the covered entity has taken action in reliance thereon. Such revocation must be in writing.

(6) A covered entity must document and retain any signed consent under this section as required by § 164.530(j).

(c) *Implementation specifications: Content requirements.* A consent under this section must be in plain language and:

(1) Inform the individual that protected health information may be used and disclosed to carry out treatment, payment, or health care operations;

(2) Refer the individual to the notice required by § 164.520 for a more complete description of such uses and disclosures and state that the individual has the right to review the notice prior to signing the consent;

(3) If the covered entity has reserved the right to change its privacy practices that are described in the notice in accordance with § 164.520(b)(1)(v)(C), state that the terms of its notice may change and describe how the individual may obtain a revised notice;

(4) State that:

(i) The individual has the right to request that the covered entity restrict how protected health information is used or disclosed to carry out treatment, payment, or health care operations;

(ii) The covered entity is not required to agree to requested restrictions; and

(iii) If the covered entity agrees to a requested restriction, the restriction is binding on the covered entity;

(5) State that the individual has the right to revoke the consent in writing, except to the extent that the covered entity has taken action in reliance thereon; and

(6) Be signed by the individual and dated.

(d) *Implementation specifications: Defective consents.* There is no consent under this section, if the document submitted has any of the following defects:

(1) The consent lacks an element required by paragraph (c) of this section, as applicable; or

(2) The consent has been revoked in accordance with paragraph (b)(5) of this section.

(e) *Standard: Resolving conflicting consents and authorizations.* (1) If a covered entity has obtained a consent under this section and receives any other authorization or written legal permission from the individual for a disclosure of protected health information to carry out treatment, payment, or health care operations, the covered entity may disclose such protected health information only in accordance with the more restrictive consent, authorization, or other written legal permission from the individual.

(2) A covered entity may attempt to resolve a conflict between a consent and an authorization or other written legal permission from the individual described in paragraph (e)(1) of this section by:

(i) Obtaining a new consent from the individual under this section for the disclosure to carry out treatment, payment, or health care operations; or

(ii) Communicating orally or in writing with the individual in order to determine the individual's preference in resolving the conflict. The covered entity must document the individual's preference and may only disclose protected health information in accordance with the individual's preference.