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

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

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

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

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

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

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

Authorizations

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

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

Training

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

Conclusion

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

TABLE 2.—THE COST OF COMPLYING WITH THE PROPOSED PRIVACY REGULATION

[In Dollars]

Provision	Initial or first year cost (2000)	Annual cost after the first year	Five year (2000–2004) cost
Development of Policies and Procedures—Providers (totaling 871,294)	$333,000,000	.....	$333,000,000
Development of Policies and Procedures—Plans (totaling 18,225)	62,000,000	.....	62,000,000
System Changes—All Entities	90,000,000	.....	90,000,000
Notice Development Cost—all entities	20,000,000	.....	30,000,000
Notice Issuance—Providers	59,730,000	37,152,000	208,340,000
Notice Issuance—Plans	46,200,000	46,200,000	231,000,000
Inspection/Copying	81,000,000	81,000,000	405,000,000
Amendment/Correction	407,000,000	407,000,000	2,035,000,000
Written Authorization	54,300,000	54,300,000	271,500,000

TABLE 2.—THE COST OF COMPLYING WITH THE PROPOSED PRIVACY REGULATION—Continued

[In Dollars]

Provision	Initial or first year cost (2000)	Annual cost after the first year	Five year (2000–2004) cost
Paperwork/Training	22,000,000	22,000,000	110,000,000
Other Costs*	**N/E	N/E	N/E
Total	1,165,230,000	647,652,000	3,775,840,000

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

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

Costs to the Federal Government

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

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

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

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

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

Costs to State Governments

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

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

existing Privacy Act rule. Further, we anticipate that most state health programs will, to some extent, need to modify their existing Privacy Act practices to fully comply with this rule.

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

F. Benefits

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

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

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

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

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

Qualitative Discussion

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

[36] John Hornberger *et al,* ''Early treatment with Highly Active Anti-Retroviral Therapy (HAART) is cost-effective compared to delayed treatment,'' 12th World AIDS conference, 1998.

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

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

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

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

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

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

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

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

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

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

G. Examination of Alternative Approaches

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

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

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

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

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

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

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

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

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

2. General Rules (§ 164.506)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

We understand that the requirements outlined in this section do not create a bright line test for determining the minimum necessary amount of protected health information appropriate for most uses or disclosures. Because of this lack of precision, we considered eliminating the requirement altogether. We also considered merely requiring covered entities to address the concept within their internal privacy

procedures, with no further guidance as to how each covered entity would address the issue. These approaches were rejected because minimizing both the amount of protected health information used and disclosed within the health care system and the number of persons who have access to such information is vital if we are to successfully enhance the confidentiality of people's personal health information. We invite comments on the approach that we have adopted and on alternative methods of implementing the minimum necessary principle.

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

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

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

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

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

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

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

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

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

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

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

We are also proposing that a business partner's use and disclosure of protected health information be limited by the terms of the business partner's contractual agreement with the covered entity. We propose that a contract between a covered entity and a business partner could not grant the business partner authority to make uses or disclosures of protected health information that the covered entity itself would not have the authority to make. The contract between a covered entity and a business partner could further limit the business partner's authority to

use or disclose protected health information as agreed to by the parties. Further, the business partner would have to apply the same limitations to its subcontractors (or persons with similar arrangements) who assist with or carry out the business partner's activities.

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

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

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

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

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

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

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

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

Our intention in this section is to recognize the myriad of business relationships that currently exist and to ensure that when they involve the exchange of protected health information, the roles and responsibilities of the different parties with respect to the protected health

information are clear. We do not propose to fundamentally alter the types of business relationships that exist in the health care industry or the manner in which they function. We request comments on the extent to which our proposal would disturb existing contractual or other arrangements among covered entities and business partners.

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

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

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

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

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

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

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

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

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

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

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

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

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

We are proposing that when covered entities initiate the authorization by asking individuals to authorize disclosure, the authorization be required to include all of the items required above as well as several additional items. We are proposing additional

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

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

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

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

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

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

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

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

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

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

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

We would restrict the discussion of discretionary disclosures to the general principles behind such disclosures rather than a detailed description of each allowable disclosure. More elaborate discussion of options for individual classes of disclosures can be found in the preamble. These disclosures are optional disclosures and therefore, any costs related to making these disclosures would incur optional costs. We do not have a complete understanding of how often these disclosures are currently made, nor do we understand what procedures are currently in place. We also do not understand how often these disclosures would be made given the new costs associated with such disclosures. Note

that the degree of new costs imposed if an entity opts to use a disclosure varies dramatically depending on the type of disclosure. For example, a disclosure of directory information in a hospital would probably not involve significant additional costs, while research that is not subject to the common could would have significant new costs involved. These disclosures, and thus these costs, are optional under this proposed rule. While they may be mandated under other law, such mandated disclosures are already being made, so there would be no additional costs. In this case there are only marginal new costs related to these disclosures.

10. Clearinghouses and the Rights of Individuals

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

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

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

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

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

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

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

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

In § 164.512, we propose the categories of information that would be required in each notice of information practices, the specific types of information that would have to be included in each category, and general guidance as to the presentation of written materials. A sample notice is provided at Appendix A of this preamble.

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

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

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

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

In proposed § 164.512, we would require each covered plan and provider to include in the notice an explanation of how it uses and discloses protected health information. The explanation must be provided in sufficient detail as to put the individual on notice of the uses and disclosures expected to be made of his or her protected health information. As explained above in section II.C.7, covered plans and providers may only use and disclose protected health information for purposes stated in this notice.

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

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

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

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

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

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

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

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

We would not require providers to mail or otherwise disseminate their notices after giving the notice to individuals at the time of the first service delivery. Providers' patient lists may include individuals they have not

served in decades. It would be difficult for providers to distinguish between ''active'' patients, those who are seen rarely, and those who have moved to different providers. While some individuals would continue to be concerned with the information practices of providers who treated them in the distant past, overall the burden of an active distribution requirement would not be outweighed by improved individual control and privacy protection.

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

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

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

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

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

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

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

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

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

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

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

The Privacy Act requires that upon receipt of a request for amendment (not access), the agency would send an acknowledgment to the individual

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

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

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

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

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

In § 164.514(d)(4), we propose that a covered plan or provider that denies an individual's request for inspection and copying in whole or in part be required to provide the individual with a written statement in plain language explaining the reason for the denial. The statement could include a direct reference to the section of the regulation relied upon for the denial, but the regulatory citation alone would not sufficiently explain the reason for the denial. The statement would need to include the name and number of the contact person or office within the entity who is responsible for receiving complaints. In addition, the statement would need to include information regarding the submission of a complaint with the Department pursuant to § 164.522(b).

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

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

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

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

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

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

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

We are proposing that the accounting include all disclosures for purposes other than treatment, payment, and health care operations, subject to certain exceptions for disclosures to law enforcement and oversight agencies, discussed below. This would also include disclosures that are authorized by the individual. The accounting would include the date of each disclosure; the name and address of the organization or person who received the protected health information; and a brief description of the information disclosed. For all disclosures that are authorized by the individual, we are proposing that the covered entity maintain a copy of the authorization form and make it available to the individual with the accounting.

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

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

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

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

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

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

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

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

We are proposing that the covered plan or provider would take action on a request for amendment or correction as quickly as the circumstances require, but not later than 60 days following the

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

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

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

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

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

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

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

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

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

15. Administrative Requirements (§ 164.518)

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

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

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

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

responsibility is privacy policy, and he or she might choose to convene a committee representing several different components of the entity to develop and implement privacy policy.

b. Training (§ 164.518(b))

In proposed § 164.518(b), we would require covered entities to provide training on the entities policies and procedures with respect to protected health information. Each entity would be required to provide initial training by the date on which this proposed rule becomes applicable. After that date, each covered entity would have to provide training to new members of the workforce within a reasonable time period after joining the entity. In addition, we are proposing that when a covered entity makes material changes in its privacy policies or procedures, it would be required to retrain those members of the workforce whose duties are directly affected by the change within a reasonable time of making the change.

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

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

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

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

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

c. Safeguards (§ 164.518(c))

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

i. *Verification procedures.*

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

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

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

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

In proposed § 164.518(d), we would require covered plans and providers to have some mechanism for receiving complaints from individuals regarding the covered plan's or provider's compliance with the requirements of this proposed rule. The covered plan or provider would be required to accept complaints about any aspect of their practices regarding protected health information. We would not require that the entity develop a formal appeals mechanism, nor that ''due process'' or any similar standard be applied. We would not require that covered entities respond in any particular manner or time frame. We are proposing two basic requirements for the complaint process. First, the covered plan or provider would be required to identify a contact person or office in the notice of information practices for receiving complaints. This person or office could either be responsible for handling the complaints or could put the individual in touch with the appropriate person within the entity to handle the particular complaint. See proposed § 164.512. This person could, but would not have to be, the entity's privacy official. See proposed § 164.518(a)(2). Second, the covered plan or provider would be required to maintain a record of the complaints that are filed and a brief explanation of the resolution, if any.

We considered requiring covered plans and providers to provide a formal internal appeal mechanism, but rejected that option as too costly and burdensome for some entities. We also considered eliminating this requirement entirely, but rejected that option because a complaint process would give covered plans or providers a way to learn about potential problems with privacy policies or practices, or training

issues. We also hope that providing an avenue for covered plans or providers to address complaints would lead to increased consumer satisfaction. We believe this approach strikes a reasonable balance between allowing covered plans or providers flexibility and accomplishing the goal of promoting attention to improvement in privacy practices. If an individual and a covered plan or provider are able to resolve the individual's complaint, there could be no need for the individual to file a complaint with the Secretary under proposed § 164.522(b). However, an individual has the right to file a complaint with the Secretary at any time. An individual could file a complaint with the Secretary before, during, after, or concurrent with filing a complaint with the covered plan or provider or without filing a complaint with the covered plan or provider.

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

e. Sanctions (§ 164.518(e))

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

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

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

f. Sanctions (§ 164.518(f))

We propose in § 164.518(f) that covered entities be required to have procedures for mitigating, to the extent practicable, any deleterious effect of a use or disclosure of protected health information by their members of their workforce or business partners. With respect to business partners, we also propose that covered entities have an affirmative duty to take reasonable steps in response to breaches of contract terms.

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

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

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

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

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

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

In an attempt to ensure that large entities develop coordinated and comprehensive policies and procedures as required by this section, we considered proposing that entities with annual receipts greater than $5

million [40] be required to have a privacy board review and approve the documentation of policies and procedures. As originally conceived, the privacy board would only serve to review research protocols as described in § 164.510(j). We believe that such a board could also serve as ''privacy experts'' for the covered entity and could review the entity's documented policies and procedures. In this capacity, the overriding objective of the board would be to foster development of up-to-date, individualized policies that enable the organization to protect health information without unnecessarily interfering with the treatment and payment functions or business needs. This type of review is particularly important for large entities who would have to coordinate policies and procedures among a large staff, but smaller organizations would be encouraged, but not required, to take a similar approach (*i.e.*, have a widely representative group participate in the development and/or review of the organization's internal privacy policies and the documentation thereof). We solicit comment on this proposal.

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

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

17. Compliance and Enforcement

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

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

V. Initial Regulatory Flexibility Analysis

A. Introduction

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

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

Reasons for Promulgating the Rule

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

Objectives and Legal Basis

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

Relevant Federal Provisions

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

B. Economic Effects on Small Entities

1. Number and Types of Small Entities Affected

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

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

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

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

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

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

We chose to use the SBA data in the RFA because we wanted our analysis to be as consistent to SBA definitions as possible to give the greatest accuracy for the RFA purposes.

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

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

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

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

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

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

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

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

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

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

[1] Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1996.
[2] The SBA defines a small business as those businesses with less than $5,000,000 in annual revenue. For consistency with the Regulation, we employ the term ''entity'' in place of ''business''.

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

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

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

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

2. Activities and Costs Associated with Compliance

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

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

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

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

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

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

[45] Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1996.
[46] Op.cit., 1996
[47] Health Care Finance Administration, OSCAR
[48] Faulkner & Gray's *Health Data Directory,* 1999
[49] International Billing Association, 1999

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The implementation of this requirement would depend on the size of the entity. For example, a small physician's practice might designate the office manager as the privacy official, and he or she would assume this as one of his or her broader administrative responsibilities. A large entity might appoint an individual whose sole responsibility is privacy policy, and that individual could choose to convene a committee representing several different components of the entity to develop and implement privacy policy.

In proposed § 164.518(b), we would require covered entities to provide training on the their policies and procedures with respect to protected health information. Entities would determine the most effective means of communicating with their workforce. For example, in a small physician practice, the training requirement could be satisfied by providing each new member of the workforce with a copy of the practice's information policies and requiring members of the workforce to acknowledge that they have reviewed the policies. A large health plan could provide for a training program with live instruction, video presentations or interactive software programs. The small physician practice's solution would not protect the large plan's data, and the plan's solution would be neither economically feasible nor necessary for the small physician practice.

In proposed § 164.518(c), we would require covered entities to put in place

administrative, technical, and physical safeguards to protect against any reasonably anticipated threats or hazards to the privacy of the information, and unauthorized uses or disclosures of the information.

In proposed § 164.518(d), we would require covered plans and providers to have some mechanism for receiving complaints from individuals regarding the covered plan's or provider's compliance with the requirements of this proposed rule. We considered requiring covered plans and providers to provide a formal internal appeal mechanism, but rejected that option as too costly and burdensome for some entities. We also considered eliminating this requirement entirely, but rejected that option because a complaint process would give covered plans or providers a way to learn about potential problems with privacy policies or practices, or training issues. We also hope that providing an avenue for covered plans or providers to address complaints would lead to increased consumer satisfaction. We believe this approach strikes a reasonable balance between allowing covered plans or providers flexibility and accomplishing the goal of promoting attention to improvement in privacy practices.

We expect that sanctions would be more formally described and consistently carried out in larger, more sophisticated entities. Smaller, less sophisticated entities would be given more latitude and flexibility. For such smaller entities and less sophisticated entities, we would not expect a prescribed sanctions policy, but would expect that actions be taken if repeated instances of violations occur. In proposed § 164.518(e), we would require all covered entities to develop and apply when appropriate sanctions for failure to comply with policies or procedures of the covered entity or with the requirements of this proposed rule.

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

3. The Burden on a Typical Small Business.

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

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

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

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

Our cost calculations are based on several assumptions. The cost of developing privacy policies is based on figures from the regulatory impact analysis that accompanied the HIPAA National Provider Identifier (63 FR 25320). The cost of initial systems compliance is based on current assumptions about market behavior; including the assumption that a relatively small proportion of the total cost of system compliance (20%) will be absorbed by small covered entities. We evaluated the ongoing costs of an entity's privacy protection by calculating that privacy protection costs should be proportional to the number of patients served by the business. For example, the cost of notifying patients of privacy practices will be directly proportional to the number of patients served. We then multiplied the proportion of small entities by the total ongoing costs of privacy compliance.

Initial Costs

Table C shows the results of our calculations of the cost of initial compliance. We calculated initial privacy policy costs separate from initial system compliance costs because we made different assumptions about the cost of each. To calculate initial privacy policy costs per small entity, we multiplied the estimated cost of developing privacy policies (per entity) by the number of establishments. We then averaged these costs and computed that the average cost of developing privacy policies is $334.31 per small entity. The average cost of implementing privacy policies is greater

than the $300 cost we assume most health care provider offices will pay, because we assume that small health plans, hospitals, and nursing and patient care services will spend between $500–$1,000 to implement privacy policies. Calculating the cost of system compliance per entity required us to estimate the percent of total system costs that each type of entity would incur. We used the $90 million figure (cited in the RIA) as the basis for distributing system compliance costs across various types of entities affected by the proposed rule. We estimated how this cost would be divided between small and large entities, and among plans, providers and clearinghouses.

TABLE C.—ANNUAL COST OF IMPLEMENTING PROVISIONS OF THE PROPOSED PRIVACY REGULATION IN THE FIRST YEAR

Industry	Initial costs				Ongoing costs			Total costs	
	Initial privacy policy costs incurred by small entities, per entity	Initial system compliance cost incurred by small entities [1], per entity	Notice development cost, per small entity	Total initial compliance cost, per small entity [2]	First year notice issuance costs for small entities, per small entity	Annual amendment and correction cost to small entities, per small entity	Annual written authorization cost to small entities, per small entity	Total annual ongoing cost in the first year, per small entity	Total annual initial and ongoing cost in the first year, per small entity
Drug Stores & Proprietary Stores [3]	$300	$131.19	$59.40	$490.58	$118.26	$768.64	$102.55	$989.45	$1,480.03
Accident & Health Insurance & Medical Service Plans [3] (Accident & Health Insurance and Hospital & Medical Service Plans)	1,000	1,939.86	203.91	3,143.77	314.02	127.60	17.02	458.65	3,602.41
Offices & Clinics Of Doctors Of Medicine	300	21.04	21.20	342.24	42.21	260.93	34.81	337.96	680.20
Offices & Clinics Of Dentists	300	7.43	13.25	320.68	26.39	163.11	21.76	211.26	531.94
Offices & Clinics Of Other Health Practitioners	300	11.10	17.82	328.92	35.47	219.29	29.26	284.02	612.94
Nursing & Personal Care Facilities	1,500	117.15	49.63	1,666.79	98.82	610.88	81.50	791.20	2,457.99
Hospitals	1,500	7,362.22	79.65	8,941.87	158.59	980.36	130.80	1,269.75	10,211.62
Home Health Care Services	300	58.06	30.66	388.72	61.05	377.38	50.35	488.77	877.49
Other Health Care Services including Lab Services	300	19.83	10.84	330.68	21.59	133.47	17.81	172.87	503.55
Average Cost	334.31	40.13	21.17	395.61	42.05	260.23	34.72	337.00	732.61

[1] The SBA defines small health care entities as those with annual revenue under $5,000,000.
[2] Total Initial Compliance Cost includes policy implementation and systems compliance costs.
[3] Includes some entities not covered by this regulation. Pharmacies are the only component of Drug Stores and Proprietary Stores covered by the regulation. Accident and workers compensation insurance are not covered by the regulation.

TABLE D.—ANNUAL COST OF IMPLEMENTING PROVISIONS OF THE PROPOSED PRIVACY REGULATION, AFTER THE FIRST YEAR

Industry	Ongoing Costs				
	Annual notice issuance costs after the first year, per small entity	Annual amendment and correction cost to small entities, per small entity	Annual written authorization cost to small entities, per small entity	Annual ongoing costs for paperwork and training, per small entity	Total annual ongoing cost after the first year, per small entity
Drug Stores & Proprietary Stores [1]	73.26	768.64	102.55	20	964.45
Accident & Health Insurance & Medical Service Plans [2] (Accident & Health Insurance and Hospital & Medical Service Plans)	314.02	127.60	17.02	60	518.65
Offices & Clinics Of Doctors Of Medicine	26.15	260.93	34.81	20	341.90
Offices & Clinics Of Dentists	16.35	163.11	21.76	20	221.22
Offices & Clinics Of Other Health Practitioners	21.97	219.29	29.26	20	290.52
Nursing & Personal Care Facilities	61.22	610.88	81.50	100	853.59
Hospitals	98.24	980.36	130.80	100	1,309.40
Home Health Care Services	37.82	377.38	50.35	20	485.54
Other Health Care Services including Lab Services	13.38	133.47	17.81	20	184.65
Average Cost	26.16	260.23	34.72	22.28	343.39

[1] The SBA defines small health care entities as those with annual revenue under $5,000,000.
[2] Includes some entities not covered by this regulation. Pharmacies are the only component of Drug Stores and Proprietary Stores covered by the regulation. Accident and workers compensation insurance are not covered by the regulation.

Our calculations regarding division of costs are based on two assumptions: (1) System costs are principally fixed costs associated with the purchase of hardware and software [50]; and (2) large entities will continue to invest more heavily in hardware and software expenditures than small entities. We estimate that 80 percent of the system costs will be born by large entities. The remaining 20 percent of total systems costs will be absorbed by small entities. To calculate the effect on small businesses, we multiplied the system compliance costs cited in the RIA by the proportion of the costs we expect small entities to incur (20 percent of total). We then multiplied the total cost of system compliance for small entities by the percentage of health care revenue by industry and calculated a cost per entity.

We used HCFA's estimate of total national health expenditures to calculate the percent of total health care business that is represented by types of health care entities. We calculated the proportion of business transacted by a type of health care entity (by SIC code) and multiplied this by the total expenditures ($1.084 billion total) [51]. National expenditure data is a useful measure for allocating system compliance costs for two reasons. Even though system compliance costs are primarily fixed costs, we assume that they bear some relationship to the size and level of the activity of the entity.

[50] We are not suggesting that these investments are exclusively computer-related. They may also include costs for personnel training, reorganization, and contract negotiations with outside entities.

[51] Health Care Finance Administration, 1996 http://www.hcfa.gov/stats/nheoact/tables/t10.htm

Similarly, national expenditures vary according to both size and level of activity. Second, in contrast to the annual receipts compiled by the Business Census Survey, national expenditure information compares its data to other sources in order to validate its results. Thus, we decided that the national expenditure data are a more reliable source of overall business activity for our purposes. Based on these assumptions, we believe that the total cost of system compliance for all small health care entities will be approximately 18 million. Dividing costs by the number of small entities suggests that the average cost of system compliance is $40.13 per entity.

The cost of notice development is approximately $21 per small entity. We assume that many small providers will receive assistance developing their notice policies from professional associations. Thus, the overall cost of developing compliant notices is significant, but the cost per entity is small. The cost to small entities of developing notices is based on the proportion of expenditures generated by small entities. We recognize that this may not adequately capture the costs of developing a provider or plan's notice of their privacy policies, and invite comment on our approach.

We added the per-entity cost of privacy policy implementation to the cost of systems compliance to determine the total average cost of start-up compliance. Our figures indicate that initial compliance will cost an average of $396 per small entity. These costs vary across entity type (Table C). For example, small hospitals have a much higher cost of compliance than the average cost for all small entities, whereas dentists' offices tend to have initial compliance costs that are lower than the average for small entities. Most small practitioner offices have low costs ($320 per dentist office), whereas small hospitals ($8,942 per entity) and small insurance companies have much higher costs ($3,144 per entity) than other health care entities.

Finally, we attempted to estimate the impact of compliance costs on small entities by comparing the cost of complying with the proposed rule to an entity's annual expenditures (Table E). We computed the percent of small entity expenditures as a percent of national expenditures by calculating the proportion of small business receipts (from census data compiled for the SBA) that apply to segments of the health care market. Although we believe that the SBA data understates the amount of annual receipts, we assumed that the underestimates are consistent across all entities. Thus, although the dollar amounts reported by the SBA are incorrect, our assumption is that the proportion of small entity receipts relative to total annual receipts is correct.

Applying the percent of small entity receipts to the national expenditure data allows us to estimate the percent of national expenditures represented by small entities. We then considered the total compliance cost (initial and ongoing cost) as a percent of small business expenditures. Our estimates suggest that the cost of complying with the proposed rule represent approximately 0.12 percent of total annual expenditures for a small health care entity in the first year. The relative cost of complying with the proposed rule is substantially lower in subsequent years, representing 0.04 percent of an entity's annual expenditures. The relative cost of complying with the proposed regulation cost of complying is highest for small health insurers (1.03 percent of expenditures). These costs will be higher due to the volume and complexity of health plan billing systems; health plans are required to implement more policies and procedures to protect health information because they handle so much personally identifiable information. Because health plan costs are higher and there is a smaller number of plans than other type of entities affected by the regulation, these costs result in a higher annual cost per small health plan. Table E further illustrates the cost impact by type of entity in the first year.

TABLE E.—SMALL ENTITY BUSINESS EXPENDITURES AND PROPORTION OF ANNUAL EXPENDITURES REPRESENTED BY INITIAL AND ONGOING COMPLIANCE COSTS IN THE FIRST YEAR*

Industry	Total annual initial and ongoing costs in the first year, per small entity	Annual expenditure per small entity [1]	Compliance cost as a percentage of a small entity's annual expenditures
Drug Stores & Proprietary Stores [2]	$1,480.03	$2,046,199	0.07
Accident & Health Insurance & Medical Service Plans [2] (Accident & Health Insurance and Hospital & Medical Service Plans)	3,602.41	350,467	1.03
Offices & Clinics Of Doctors Of Medicine	680.20	695,560	0.10
Offices & Clinics Of Dentists	531.94	434,260	0.12
Offices & Clinics Of Other Health Practitioners	612.94	583,805	0.10
Nursing & Personal Care Facilities	2,457.99	1,629,755	0.15
Hospitals	10,211.62	2,660,215	0.38
Home Health Care Services	877.49	1,003,475	0.09
Other Health Care Services including Lab Services	503.55	351,146	0.14
Average Cost	732.61	625,992	0.12

* The SBA defines small health care entities as those with annual revenue under $5,000,000.
** Total Initial Compliance Cost includes policy implementation and systems compliance costs
[1] Based on the assumption that the proportion of revenue generated by small businesses approximates the proportion of expenditures faced by small businesses
[2] Includes some entities not covered by this regulation. Pharmacies are the only component of Drug Stores and Proprietary Stores covered by the regulation. Accident and workers compensation insurance are not covered by the regulation.

Ongoing Costs

In this section, we evaluate the ongoing costs of providing patient notices, the annual cost of amending and correcting medical information, the cost of providing written authorizations, and the ongoing cost of paperwork and training. We estimated the ongoing costs of compliance through calculations

similar to those used for our systems compliance estimates. Ongoing costs are most heavily influenced by the size of the business. Therefore, we assume that the number of patients an entity serves is directly proportional to its ongoing compliance costs.

We estimated market share using Small Business Administration data estimating total receipts.[52] We divided the small entity receipts by total receipts and arrived at an estimate that 22 percent of the revenue generated by the health care classifications we examined is from small businesses. Using annual receipts to estimate cost burden is more accurate than using information on the number of health care entities. The size of the small entity is more likely to be correlated with the number of patients served than the number of businesses, and therefore, the amount of business conducted by an entity. Because it is difficult to find a single good estimate of market share, we considered estimating market share over a range, using the proportion of annual receipts as a lower bound and number of entities as the higher bound. We concluded that even if the SBA data does not capture the total amount of health care receipts accurately, estimating market share by examining receipts would be much more accurate than using the number of entities.

We multiplied the percent total receipts by the total ongoing costs (by entity type) to obtain a range of ongoing costs for small entities. We were then able to divide these costs by the number of small entities by type of entity. We estimated ongoing costs in the first year that the proposed rule takes effect separately from our estimate of ongoing cost in the following years. The estimates were approximately the same; $337 and $343 respectively.

We estimate that the ongoing cost of compliance will be approximately 0.05 percent of a small entity's annual expenditures. This cost burden is fairly consistent across all types of entities.

Clearinghouses and Nonprofit Entities

We should note that the above discussion does not consider health care clearinghouses, nonprofit hospitals, home health agencies, or nursing and skilled nursing facilities. To the extent that clearinghouses and nonprofit facilities have annual receipts of less than $5 million, they were included in the preceding analysis.

Although we do not have precise information on the number of clearinghouses that qualify as small entities under the RFA, we believe that approximately half would meet the criteria. As noted in the regulatory impact analysis, as long as clearinghouses perform the function of merely reformatting information they receive and transmitting the data to other entities, the cost of complying with the proposed rule should be minimal.

A similar logic applies for nonprofit health plans and hospitals. We do know how many nonprofit organizations currently exist in the U.S., but do not have reliable revenue and expenditure data for these entities. In the absence of such data, we assume that nonprofit entities have a similar ratio of revenues to expenditures as the for-profit entities we have examined. Thus, we believe that the impact of complying with the proposed rule should be similar to that described for-profit plans and hospitals.

The preceding analysis indicates that the expected burden on small entities of implementing the proposed rule would be minimal. However, by necessity, the analysis is based on average costs, and as such, they may not reflect the actual burden on some or even a substantial number of small entities. Therefore, the Secretary does not certify that the proposed rule will not have a significant impact on a substantial number of small entities.

VI. Unfunded Mandates

The Unfunded Mandates Reform Act of 1995 (Pub. L. 104–4) requires cost-benefit and other analyses for rules that would cost more than $100 million in a single year. The proposed rule qualifies as a significant rule under the statute. DHHS has carried out the cost-benefit analysis in sections D and E of this document, which includes a discussion of unfunded costs to the states resulting from this regulation.

A. Future Costs

DHHS estimates some of the future costs of the proposed rule in Section E of the Preliminary Regulatory Impact Analysis of this document. The reported costs include costs incurred during the compliance period and up to 5 years after the effective date. The same section also includes some qualitative discussion of costs that would occur beyond that time period. Most of the costs of the proposed rule, however, would occur in the years immediately after the publication of a final rule. Future costs beyond the five year period will continue but will not be as great as the initial compliance costs.

B. Particular Regions, Communities, or Industrial Sectors.

The proposed rule applies to the health care industry and would, therefore, affect that industry disproportionately. Any long-run increase in the costs of health care services would largely be passed on to the entire population of consumers.

C. National Productivity and Economic Growth

The proposed rule is not expected to substantially affect productivity or economic growth. It is possible that productivity and growth in certain sectors of the health care industry could be slightly lower than otherwise because of the need to divert research and development resources to compliance activities. The diversion of resources to compliance activities would be temporary. Moreover, DHHS anticipates that, because the benefits of privacy are large, both productivity and economic growth would be higher than in the absence of the proposed rule. In section I.A. of this document, DHHS discusses its expectation that this proposed rule would increase communication among consumers, health plans, and providers and that implementation of privacy protections will lead more people to seek health care. The increased health of the population will lead to increased productivity and economic growth.

D. Full Employment and Job Creation.

Some of the human resources devoted to delivery of health care services would be redirected by the proposed rule. The proposed rule could lead to some short-run changes in employment patterns as a result of the structural changes within the health care industry. The growth of employment (job creation) for the roles typically associated with the health care profession could also be temporarily change but be balanced by an increased need for those who can assist entities with complying with this proposed rule. Therefore, while there could be a temporary slowing of growth in traditional health care professions, that will be offset by a temporary increase in growth in fields that may assist with compliance with this proposed rule (e.g. legal professionals, and management consultants).

E. Exports

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

VII. Environmental Impact

The Department has determined under 21 CFR 25.30(K) that this action

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

is of a type that does not individually or cumulatively have a significant effect on the human environment. Therefore, neither an environmental assessment nor an environmental impact statement is required.

VIII. Collection of Information Requirements

Under the Paperwork Reduction Act of 1995 (PRA), agencies are required to provide a 60-day notice in the **Federal Register** and solicit public comment before a collection of information requirement is submitted to the Office of Management and Budget (OMB) for review and approval. In order to fairly evaluate whether an information collection should be approved by OMB, section 3506(c)(2)(A) of the PRA requires that we solicit comment on the following issues:

- Whether the information collection is necessary and useful to carry out the proper functions of the agency;
- The accuracy of the agency's estimate of the information collection burden;
- The quality, utility, and clarity of the information to be collected; and
- Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

Under the PRA, the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section are to be considered. Due to the complexity of this regulation, and to avoid redundancy of effort, we are referring readers to Section IV (Regulatory Impact Analysis) above, to review the *detailed* cost assumptions associated with these PRA requirements. We explicitly seek, and will consider public comment on our cost assumptions, as they relate to the PRA requirements summarized in this section.

SUMMARY PRA BURDEN HOURS

Provision	Burden (in hours)
§ 160.204 Process for requesting exceptions.	160
§ 164.506 General standards and implementation specifications for uses and disclosures of protected health information.	*TBD
§ 164.508 Standards and implementation specifications for uses and disclosures for which individual authorization would be required.	3,561,076
§ 164.510 Standards and implementation specifications for uses and disclosures for which individual authorization would not be required.	8,903
§ 164.512 Notice of privacy practices; rights and procedures.	7,273,952
§ 164.514 Access to protected health information; rights and procedures.	*TBD
§ 164.515 Accounting for uses and disclosures of protected health information	*TBD
§ 164.516 Amendment and correction; rights and procedures	*TBD
§ 164.520 Development and documentation of policies and procedures	2,927,000
§ 164.522 Compliance and Enforcement	2,500
Total Hours	13,773,591

*Burden to be determined based upon public comment.

Section 160.204 Process for Requesting Exceptions.

Section 160.204 would require States to: (1) Submit a written request, that meets the requirements of this section, to the Secretary to except a provision of State law from preemption under § 160.203; (2) submit a new request to the Secretary, should there be any changes to the standard, requirement, or implementation specification or provision of State law upon which an exception previously was granted, and (3) submit a written request for an extension of the exception prior to the end of the three-year approval period for a given exception. In addition, § 160.204 would require a State to submit a written request for an advisory opinion to the Secretary that meets the requirements of § 160.204.

The burden associated with these requirements is the time and effort necessary for a State to prepare and submit the written request for preemption or advisory opinion to HCFA for approval. On an annual basis it is estimated that it will take 10 States 16 hours each to prepare and submit a request. The total annual burden associated with this requirement is 160 hours.

Section 164.506 General Standards and Implementation Specifications for Uses and Disclosures of Protected Health Information

Given that the burden associated with the following information collection requirements will differ significantly, by the type and size of plan or provider, we are explicitly soliciting comment on the burden associated with the following requirements:

- Except for disclosures of protected health information by a covered entity that is a health care provider to another health care provider for treatment purposes, § 160.204(e) would require a covered entity to maintain documentation demonstrating that they have entered into a contract that meets the requirements of this part with each of their business partners;
- A covered entity would have to make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose of the use or disclosure;
- A covered entity could use protected health information to create de-identified information if the individually identifiable information has been removed, coded, encrypted, or otherwise eliminated or concealed.

Section 164.508 Standards and Implementation Specifications for Uses and Disclosures for Which Individual Authorization Would Be Required

Pursuant to the conditions set forth in this section, a covered entity would need to obtain a written request from an individual, before it uses or discloses protected health information of an individual. A copy of the model form which appears in Appendix to Subpart E of Part 164, or a form that contains the elements listed in paragraphs (c) or (d) of this section, as applicable, would need to be accepted by the covered entity.

The burden associated with these proposed requirements is the time and effort necessary for a covered entity to obtain written authorization prior to the disclosure of identifiable information. On an annual basis it is estimated that it will take 890,269 entities, a range of 0 to 80 hours per entity to obtain and

maintain authorization documentation on an annual basis. Given that we believe the majority of the covered entities will be minimally affected by this requirement, we estimate the annual average burden per entity to be 4 hours for a total annual burden of 3,561,076 hours. Collecting such authorization should have costs on the order of those associated with providing access to records (not on a per page basis). Since the proposed requirement does not apply to treatment and payment, assuming 1% of the 543 million health care encounters might be reasonable. At a cost of about $10 each, the aggregate cost would be about $54 million. Therefore, on average the cost per entity would be about $60, with many entities receiving no requests and thus having no costs.

Section 164.510 Standards and Implementation Specifications for Uses and Disclosures for Which Individual Authorization Would Not Be Required

A covered entity could disclose protected health information to a health researcher for health research purposes subject to 45 CFR part 46 and purposes other than those subject to 45 CFR part 46, provided that the covered entity has obtained written documentation demonstrating that the applicable requirements proposed in this section have been met.

The burden associated with these proposed requirements is the time and effort necessary for a covered entity to maintain documentation demonstrating that they have obtained institutional review board or privacy board approval, which meet the requirements of this section. On an annual basis it is estimated that this proposed requirement will affect 1 % or 8,903 of covered entities. We further estimate that it will take an average of 1 hour per entity to meet these proposed requirements on an annual basis. Therefore, the total estimated annual burden associated with this proposed requirement is 8,903 hours.

Section 164.512 Notice of Privacy Practices; Rights and Procedures

Section 164.512 would require covered entities to provide written notice of the entities' privacy practices, rights, and procedures that meet the requirements of this section to affected parties upon request and as summarized below.

Health plans would provide a copy of the notice to an individual covered by the plan at enrollment and whenever the content of the notice is significantly altered thereafter, but no less frequently than once every three years. Total notice counts are estimated to be about 230 million, assuming plans choose to send them out annually rather than keeping track of duration since last notice. The average number of notices per plan per year would be about 1,200. For the approximately 19,000 plans issuing notices, the number of notices can be as few as 1,000 for a small self-insured self-administered employer, or as many as a million or more for a large commercial insurer or HMO. We further estimate that it will require each plan, on average, 8 hours to disseminate the required notices. This estimate is based upon the assumption that the required notice will be incorporated and disseminated with a plan's annual policy materials. The total burden associated with this requirement is calculated to be 151,800 hours.

Health care providers would provide a copy of the notice to an individual at the time of first service delivery to the individual, provide as promptly as possible a copy of the notice to an individual served by the provider whenever the content of the notice is significantly altered, post a copy of the notice in a location where it is reasonable to expect individuals seeking services from the provider to be able to read the notice, and date each version of the notice. Total notices in the first year are estimated to be about 700 million (based on annual patient contacts with hospitals, physicians, and other providers), with subsequent year counts of 350 million. Small providers could be providing 400 or fewer notices (based on 150 million persons with ambulatory physician contacts per year and approximately 370,000 physician offices). The overall average will also be close to that amount, since the bulk of providers are small entities. Large providers could be sending out 3,000 or more notices (based on 20 million persons with hospitalizations and approximately 6600 hospitals). We further estimate that it will require each provider, on average, 8 hours to disseminate the required notices. This estimate is based upon the assumption that the required notice will be incorporated into and disseminated with other patient materials. The total burden associated with this requirement is calculated to be 7,122,152 hours.

Section 164.514 Access of Individuals to Protected Health Information

Given that the burden associated with the following information collection requirements will differ significantly, by the type and size of plan or provider, we are explicitly soliciting comment on the burden associated with the following proposed requirements:

- An individual has a right of access to, which includes a right to inspect and obtain a copy of, his or her protected health information in a designated record set of a covered entity that is a health plan or a health care provider, including such information in a business partner's designated record set that is not a duplicate of the information held by the provider or plan, for so long as the information is maintained;
- Where the request is denied in whole or in part, the health plan or a health care provider would provide the individual with a written statement of the basis for the denial and a description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.518 or to the Secretary pursuant to the procedures established in § 164.522 of this subpart.

Section 164.515 Accounting for Uses and Disclosures of Protected Health Information

Given that the burden associated with maintaining records to facilitate the recreation of disclosures will differ significantly, be the type and size of plan or provider, we are explicitly soliciting comment on the burden associated with the following proposed record keeping requirement:

- A covered entity that is a plan or provider would need to be able to give individuals an accurate accounting of all uses and disclosures that are for purposes other than treatment, payment, and health care operations; except that such procedures would provide for the exclusion from such accounting of protected health information which is disclosed to a health oversight or law enforcement agency, if the health oversight or law enforcement agency provides a written request stating that the exclusion is necessary because disclosure would be reasonably likely to impede the agency's activities and specifies the time for which such exclusion is required.

Section 164.516 Amendment and Correction

Given that burden will associated with the following information collection requirements will differ significantly, by the type and size of plan or provider, we are explicitly soliciting comment on the burden associated with the following proposed requirements:

- An individual would have the right to request amendment or correction of his or her protected health information in designated records created by a covered entity that is a health plan or health care provider, where the

individual asserts that the information is not accurate or complete and where the error or omission may have an adverse effect on the individual.

- Where the request is denied , provide the individual with a written statement of the basis for the denial, a description of how the individual may file a statement of disagreement with the denial, a description of how the individual may file a complaint with the covered entity, including the name and telephone number of a contact person within the covered entity who can answer questions concerning the denial and the complaint process; and a description of how the individual may file a complaint with the Secretary pursuant to § 164.522 of this subpart.

Section 164.520 Internal Privacy Practices; Standards and Procedures

A covered entity would need to ensure that all employees who have access to protected health information have received appropriate training about the entity's policies for use and disclosure of such information. Upon completion of the training and at least once every three years thereafter, covered entities would require each employee to sign a statement that he or she received the privacy training and will honor all of the entity's privacy policies and procedures.

The burden associated with these requirements is the time and effort necessary for a covered entity to obtain and maintain certification documentation demonstrating that applicable employees have received privacy training and will honor all of the entity's privacy policies and procedures. It is estimated that it will take 890,269 entities, a range of 1 hour to 40 hours per entity to obtain and maintain documentation on an annual basis. Given that we believe the majority of the covered entities will be minimally affected by this requirement, we estimate the annual average burden to be 3 hours per entity for a total annual burden of 2,700,000 hours. Using previous calculations, 900,000 (rounded) entities break down to about 95% small, 5% various types of large, and 1 burden hour for 95%, and 40 burden hours for 5%, the average burden would be 3 hours.

In addition, this section would require a covered entity that is a health plan or health care provider to develop and document its policies and procedures for implementing the requirements of this proposed rule, and amend the documentation to reflect any change to a policy or procedure.

The burden associated with these requirements is the time and effort necessary for a covered entity to maintain documentation demonstrating that they have implemented procedures that meet the requirements of this proposed rule. It is estimated that it will take 890,269 entities a range of 15 minutes to 1 hour per entity to maintain procedural documentation on an annual basis. We believe the majority (95%) of the covered entities will be minimally affected by this requirement. Using the 95% small/5% large, the average burden is 17 minutes. Multiplying by 890,269, results in a total annual burden of 256,000 hours (see discussion below).

Since the requirements for developing formal processes and documentation of procedures mirror what will already have been required under the HIPAA security regulations, the burden and additional costs should be small. To the extent that national or state associations will develop guidelines or general sets of processes and procedures which will be reviewed by individual member entity, the costs would be primarily those of the individual reviewers. Assuming this process occurs, we believe that entities will review information from associations in each state and prepare a set of written policies to meet their needs. Our estimates are based on assumed costs for providers ranging from $300 to $3000, with the average being about $375. The range correlates to the size and complexity of the provider. With less than 1 million provider entities, the aggregate cost would be on the order of $300 million. For plans and clearinghouses, our estimate assumes that the legal review and development of written policies will be more costly because of the scope of their operations. They are often dealing with a large number of different providers and may be dealing with requirements from multiple states. We believe the costs for these entities will range from $300 for smaller plans to $15,000 for the largest plans. Because there are very few large plans in relation to the number of small plans, the average implementation costs will be about $3050.

Section 164.522 Compliance and Enforcement

An individual who believes that a covered entity is not complying with the requirements of this subpart may file a complaint with the Secretary within 180 days from the date of the alleged non-compliance, unless the time for filing is extended by the Secretary. The complaint would describe in detail the acts or omissions believed to be in violation of the requirements of this subpart.

The burden associated with these requirements is the time and effort necessary for an individual to prepare and submit a written complaint to the Secretary. On an annual basis it is estimated that 10,000 complaints will be filed on an annual basis. We further estimate that it will take an average of 15 minutes per individual to submit a complaint. Therefore, the total estimated annual burden associated with this requirement is 2,500 hours.

A covered entity would need to maintain documentation necessary for the Secretary to ascertain whether the covered entity has complied or is complying with the requirements of this subpart. While this section is subject to the PRA, the burden associated with this requirement is addressed under sections referenced above, which discuss specific record keeping requirements.

We have submitted a copy of this proposed rule to OMB for its review of the information collection requirements in §§ 160.204, 164.506, 164.508, 164.510, 164.512, 164.514, 164.515, 164.516, 164.520, and § 164.522. These requirements are not effective until they have been approved by OMB.

If you comment on any of these information collection and record keeping requirements, please mail copies directly to the following:

Health Care Financing Administration, Office of Information Services, Information Technology Investment Management Group, Division of HCFA Enterprise Standards, Room C2–26–17, 7500 Security Boulevard, Baltimore, MD 21244–1850. ATTN: John Burke HIPAA Privacy-P

Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10235, New Executive Office Building, Washington, DC 20503. ATTN: Allison Herron Eydt, HCFA Desk Officer.

IX. Executive Order 12612: Federalism

The Department has examined the effects of provisions in the proposed privacy regulation on the relationship between the Federal government and the States, as required by Executive Order 12612 on ''Federalism.'' The agency concludes that preempting State or local proposed rules that provide less stringent privacy protection requirements than Federal law is consistent with this Executive Order. Overall, the proposed rule attempts to balance both the autonomy of the States with the necessity to create a Federal benchmark to preserve the privacy of personally identifiable health information.

It is recognized that the States generally have laws that relate to the privacy of individually identifiable health information. The HIPAA statute dictates the relationship between State law and this proposed rule. Except for laws that are specifically exempted by the HIPAA statute, State laws continue to be enforceable, unless they are contrary to Part C of Title XI of the standards, requirements, or implementation specifications adopted or pursuant to subpart x. However, under section 264(c)(2), not all contrary provisions of State privacy laws are preempted; rather, the law provides that contrary provisions that are also ''more stringent'' than the federal regulatory requirements or implementation specifications will continue to be enforceable.

Section 3(b) of Executive Order 12612 recognizes that Federal action limiting the discretion of State and local governments is appropriate ''where constitutional authority for the action is clear and certain and the national activity is necessitated by the presence of a problem of national scope.'' Personal privacy issues are widely identified as a national concern by virtue of the scope of interstate health commerce. HIPAA's provisions reflect this position. HIPAA attempts to facilitate the electronic exchange of financial and administrative health plan transactions while recognizing challenges that local, national, and international information sharing raise to confidentiality and privacy of health information.

Section 3(d)(2) of the Executive Order 12612 requires that the Federal government refrain from ''establishing uniform, national standards for programs and, when possible, defer to the States to establish standards.'' HIPAA requires HHS to establish standards, and we have done so accordingly. This approach is a key component of the proposed privacy rule, and it adheres to Section 4(a) of Executive Order 12612, which expressly contemplates preemption when there is a conflict between exercising State and Federal authority under Federal statute. Section 262 of HIPAA enacted Section 1178 of the Social Security Act, developing a ''general rule'' that State laws or provisions that are contrary to the provisions or requirements of Part C of Title XI, or the standards or implementation specifications adopted, or established thereunder are preempted. Several exceptions to this rule exist, each of which is designed to maintain a high degree of State autonomy.

Moreover, Section 4(b) of the Executive Order authorizes preemption of State law in the Federal rule making context when there is ''firm and palpable evidence compelling the conclusion that the Congress intended to delegate to the * * * agency the authority to issue regulations preempting State law.'' Section 1178 (a)(2)(B) of HIPAA specifically preempts State laws related to the privacy of individually identifiable health information unless the State law is more stringent. Thus, we have interpreted State and local laws and regulations that would impose less stringent requirements for protection of individually identifiable health information as undermining the agency's goal of ensuring that all patients who receive medical services are assured a minimum level of personal privacy. Particularly where the absence of privacy protection undermines an individual's access to health care services, both the personal and public interest is served by establishing Federal rules.

The proposed rule would establish national minimum standards with respect to the collection, maintenance, access, transfer, and disclosure of personally identifiable health information. The Federal law will preempt State law only where State and Federal laws are ''contradictory'' and the Federal regulation is judged to establish ''more stringent'' privacy protections than State laws.

As required by the Executive Order, States and local governments will be given, through this notice of proposed rule making, an opportunity to participate in the proceedings to preempt State and local laws (section 4(e) of Executive Order 12612). However, it should be noted that the preemption of state law is based on the HIPAA statute. The Secretary will also provide a review of preemption issues upon requests from States. In addition, under the Order, appropriate officials and organizations will be consulted before this proposed action is implemented (section 3(a) of Executive Order 12612).

Finally, we have considered the cost burden that this proposed rule would impose on State-operated health care entities, Medicaid, and other State health benefits programs. We do not have access to reliable information on the number of State-operated entities and programs, nor do we have access to data on the costs these entities and programs would incur in order to comply with the proposed rule. A discussion of possible compliance costs that covered entities may incur is contained in the Unfunded Mandates section above. We believe that requiring State health care entities covered by the proposed rule to comply with the proposed rule would cost less than one percent of a State's annual budget.

The agency concludes that the policy proposed in this document has been assessed in light of the principles, criteria, and requirements in Executive Order 12612; that this policy is not inconsistent with that Order; that this policy will not impose significant additional costs and burdens on the States; and that this policy will not affect the ability of the States to discharge traditional State governmental functions.

During our consultation with the States, representatives from various State agencies and offices expressed concern that the proposed regulation would pre-empt all State privacy laws. As explained in this section, the regulation would only pre-empt state laws where there is a direct conflict between state laws and the regulation, and where the regulation provides more stringent privacy protection than State law. We discussed this issue during our consultation with State representatives, who generally accepted our approach to the preemption issue. During the consultation, we requested further information from the States about whether they currently have laws requiring that providers have a ''duty to warn'' family members or third parties about a patient's condition other than in emergency circumstances. Since the consultation, we have not received additional comments or questions from the States.

X. Executive Order 13086: Consultation and Coordination with Indian Tribal Governments

In drafting the proposed rule, the Department consulted with representatives of the National Congress of American Indians and the National Indian Health Board, as well as with a representative of the self-governance Tribes. During the consultation, we discussed issues regarding the application of Title II of HIPAA to the Tribes, and potential variations based on the relationship of each Tribe with the IHS for the purpose of providing health services. Participants raised questions about the status of Tribal laws regarding the privacy of health information.

List of Subjects in 45 CFR Parts 160 and 164

Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Medicaid, Medical

research, Medicare, Privacy, Reporting and recordkeeping requirements, security measures.

Note to reader: This proposed rule is one of several proposed rules that are being published to implement the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996. We propose to establish a new 45 CFR subchapter C, parts 160 through 164. Part 160 will consist of general provisions, part 162 will consists of the various Administrative Simplification regulations relating to transactions and identifiers, and part 164 will consists of the regulations implementing the security and privacy requirements of the legislation. Proposed part 160, consisting of two subparts (Subpart A General Provisions, and Subpart B—Preemption of State Law) will be exactly the same in each rule, unless we add new sections or definitions to incorporate additional general information in the later rules.

Dated: October 26, 1999.

Donna Shalala,

Secretary.

Appendix to the Preamble: Sample Contact of Provider Notice

PROVIDER NOTICE OF INFORMATION PRACTICES (as of 1/1/1999)

Uses and Disclosures of Health Information

We use health information about you for treatment, to obtain payment for treatment, for administrative purposes, and to evaluate the quality of care that you receive.

We may use or disclose identifiable health information about you without your authorization for several other reasons. Subject to certain requirements, we may give out health information without your authorization for public health purposes, for auditing purposes, for research studies, and for emergencies. We provide information when otherwise required by law, such as for law enforcement in specific circumstances. In any other situation, we will ask for your written authorization before using or disclosing any identifiable health information about you. If you choose to sign an authorization to disclose information, you can later revoke that authorization to stop any future uses and disclosures.

We may change our policies at any time. Before we make a significant change in our policies, we will change our notice and post the new notice in the waiting area and in each examination room. You can also request a copy of our notice at any time. For more information about our privacy practices, contact the person listed below.

Individual Rights

In most cases, you have the right to look at or get a copy of health information about you that we use to make decisions about you. If you request copies, we will charge you $0.05 (5 cents) for each page. You also have the right to receive a list of instances where we have disclosed health information about you for reasons other than treatment, payment or related administrative purposes. If you believe that information in your record is incorrect or if important information is missing, you have the right to request that we correct the existing information or add the missing information.

You may request in writing that we not use or disclose your information for treatment, payment and administrative purposes except when specifically authorized by you, when required by law, or in emergency circumstances. We will consider your request but are not legally required to accept it.

Complaints

If you are concerned that we have violated your privacy rights, or you disagree with a decision we made about access to your records, you may contact the person listed below. You also may send a written complaint to the U.S. Department of Health and Human Services. The person listed below can provide you with the appropriate address upon request.

Our Legal Duty

We are required by law to protect the privacy of your information, provide this notice about our information practices, and follow the information practices that are described in this notice.

If you have any questions or complaints, please contact: Office Administrator, 111 Main Street, Suite 101, Anytown, OH 41111. Phone: (111) 555–6789, Email: admin@docshop.com.

For the reasons set forth in the preamble, it is proposed to amend 45 CFR subtitle A by adding a new subchapter C, consisting of parts 160 through 164, to read as follows:

SUBCHAPTER C—ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS

Part

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

Subpart A—General Provisions

Sec.

Subpart B—Preemption of State Law

Authority: 42 U.S.C. 1320d–2 and 1320d–4.

Subpart A—General Provisions

§ 160.101 Statutory basis and purpose.

The requirements of this subchapter implement sections 1171 through 1179 of the Social Security Act, as amended, which require HHS to adopt national standards to enable the electronic exchange of health information in the health care system. The requirements of this subchapter also implement section 264 of Pub. L 104–191, which requires that HHS adopt national standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a)(1) of the Social Security Act. The purpose of these provisions is to promote administrative simplification.

§ 160.102 Applicability.

Except as otherwise provided, the standards, requirements, and implementation specifications adopted or designated under the parts of this subchapter apply to any entity that is:

(a) A health plan;

(b) A health care clearinghouse; and

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

§ 160.103 Definitions.

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

Act means the Social Security Act, as amended.

Covered entity means an entity described in § 160.102.

Health care means the provision of care, services, or supplies to a patient and includes any:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure with respect to the physical or mental condition, or functional status, of a patient or affecting the structure or function of the body;

(2) Sale or dispensing of a drug, device, equipment, or other item pursuant to a prescription; or

(3) Procurement or banking of blood, sperm, organs, or any other tissue for administration to patients.

Health care clearinghouse means a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. The entity receives health care transactions from health care providers or other entities, translates the data from a given format into one acceptable to the intended payer or payers, and forwards the processed transaction to appropriate payers and clearinghouses. Billing services, repricing companies, community health management information systems, community health information systems, and ''value-added''

networks and switches are considered to be health care clearinghouses for purposes of this part, if they perform the functions of health care clearinghouses as described in the preceding sentences.

Health care provider means a provider of services as defined in section 1861(u) of the Act, a provider of medical or health services as defined in section 1861(s) of the Act, and any other person or organization who furnishes, bills, or is paid for health care services or supplies in the normal course of business.

Health information means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Health plan means an individual or group plan that provides, or pays the cost of, medical care. Such term includes, when applied to government funded or assisted programs, the components of the government agency administering the program. ''Health plan'' includes the following, singly or in combination:

(1) A group health plan, defined as an employee welfare benefit plan (as currently defined in section 3(1) of the Employee Retirement Income and Security Act of 1974, 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg–91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance or otherwise, that:

(i) Has 50 or more participants; or

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

(2) A health insurance issuer, defined as an insurance company, insurance service, or insurance organization that is licensed to engage in the business of insurance in a State and is subject to State or other law that regulates insurance.

(3) A health maintenance organization, defined as a federally qualified health maintenance organization, an organization recognized as a health maintenance organization under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such a health maintenance organization.

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

(5) The Medicaid program under title XIX of the Act.

(6) A Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss).

(7) A long-term care policy, including a nursing home fixed-indemnity policy.

(8) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

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

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

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

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

(13) The Federal Employees Health Benefits Program under 5 U.S.C. chapter 89.

(14) An approved State child health plan for child health assistance that meets the requirements of section 2103 of the Act.

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

(16) Any other individual or group health plan, or combination thereof, that provides or pays for the cost of medical care.

Secretary means the Secretary of Health and Human Services and any other officer or employee of the Department of Health and Human Services to whom the authority involved has been delegated.

Small health plan means a health plan with annual receipts of $5 million or less.

Standard means a prescribed set of rules, conditions, or requirements concerning classification of components, specification of materials, performance or operations, or delineation of procedures, in describing products, systems, services or practices.

State includes the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

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

(1) Health claims or equivalent encounter information;

(2) Health care payment and remittance advice;

(3) Coordination of benefits;

(4) Health claims status;

(5) Enrollment and disenrollment in a health plan;

(6) Eligibility for a health plan;

(7) Health plan premium payments;

(8) Referral certification and authorization;

(9) First report of injury;

(10) Health claims attachments; and

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

§ 160.104 Effective dates of a modification to a standard or implementation specification.

The Secretary may modify a standard or implementation specification after the first year in which the standard or implementation specification is required to be used, but not more frequently than once every 12 months. If the Secretary adopts a modification to a standard or implementation specification, the implementation date of the modified standard or implementation specification may be no earlier than 180 days following the adoption of the modification. The Secretary will determine the actual date, taking into account the time needed to comply due to the nature and extent of the modification. The Secretary may extend the time for compliance for small health plans.

Subpart B—Preemption of State Law

§ 160.201 Applicability.

The provisions of this subpart apply to determinations and advisory opinions issued by the Secretary pursuant to 42 U.S.C. 1320d–7.

§ 160.202 Definitions.

For the purpose of this subpart, the following terms have the following meanings:

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A party would find it impossible to comply with both the State and federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104–191, as applicable.

More stringent means, in the context of a comparison of a provision of State

law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a law which meets one or more of the following criteria, as applicable:

(1) With respect to a use or disclosure, provides a more limited use or disclosure (in terms of the number of potential recipients of the information, the amount of information to be disclosed, or the circumstances under which information may be disclosed).

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

(3) With respect to penalties, provides greater penalties.

(4) With respect to information to be provided to an individual about a proposed use, disclosure, rights, remedies, and similar issues, provides the greater amount of information.

(5) With respect to form or substance of authorizations for use or disclosure of information, provides requirements that narrow the scope or duration, increase the difficulty of obtaining, or reduce the coercive effect of the circumstances surrounding the authorization.

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

(7) With respect to any other matter, provides greater privacy protection for the individual.

Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or the effect of affecting the privacy of health information in a direct, clear, and substantial way.

State law means a law, decision, rule, regulation, or other State action having the effect of law.

§ 160.203 General rule and exceptions.

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

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

(1) Is necessary:

(i) To prevent fraud and abuse;

(ii) To ensure appropriate State regulation of insurance and health plans;

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

(iv) For other purposes related to improving the Medicare program, the Medicaid program, or the efficiency and effectiveness of the health care system; or

(2) Addresses controlled substances.

(b) The provision of State law relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

(c) The provision of State law, or the State established procedures, are established under a State law providing for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification.

§ 160.204 Process for requesting exception determinations or advisory opinions.

(a) *Determinations.* (1) A State may submit a written request to the Secretary to except a provision of State law from preemption under § 160.203(a). The request must include the following information:

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

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

(iii) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;

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

(v) The length of time for which the exception would be in effect, if less than three years;

(vi) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and

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

(2) Requests for exception under this section must be submitted to the Secretary at an address which will be published in the **Federal Register**. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.

(3) The Secretary's determination under this paragraph will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met. If it is determined that the federal standard, requirement, or implementation specification accomplishes the purposes of the criterion or criteria at § 160.203(a) as well as or better than the State law for which the request is made, the request will be denied.

(4) An exception granted under this paragraph is effective for three years or for such lesser time as is specified in the determination granting the request.

(5) If an exception is granted under this paragraph, the exception has effect only with respect to transactions taking place wholly within the State for which the exception was requested.

(6) Any change to the standard, requirement, or implementation specification or provision of State law upon which an exception was granted requires a new request for an exception. Absent such a request and a favorable determination thereon, the standard, requirement, or implementation specification remains in effect. The responsibility for recognizing the need for and making the request lies with the original requestor.

(7) The Secretary may seek changes to a standard, requirement, or implementation specification based on requested exceptions or may urge the requesting State or other organizations or persons to do so.

(8) Determinations made by the Secretary pursuant to this paragraph will be published annually in the **Federal Register**.

(b) *Advisory opinions.*—(1) The Secretary may issue advisory opinions as to whether a provision of State law constitutes an exception under § 160.203(b) to the general rule of preemption under that section. The Secretary may issue such opinions at the request of a State or at the Secretary's own initiative.

(2) A State may submit a written request to the Secretary for an advisory opinion under this paragraph. The

request must include the following information:

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

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

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

(iv) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets the criteria at § 160.203(b); and

(v) Any other information the Secretary may request in order to issue the advisory opinion.

(3) The requirements of paragraphs (a)(2), (a)(5)–(a)(7) of this section apply to requests for advisory opinions under this paragraph.

(4) The Secretary's decision under this paragraph will be made on the basis of the extent to which the information provided and other factors demonstrate that the criteria at § 160.203(b) are met.

(5) Advisory opinions made by the Secretary pursuant to this paragraph will be published annually in the **Federal Register**.

PARTS 161–163—[RESERVED]

PART 164—SECURITY AND PRIVACY

Subpart A—General Provisions

Subparts B–D—[Reserved]

Subpart E—Privacy of Individually Identifiable Health Information

Authority: 42 U.S.C. 1320d–2 and 1320d–4.

Subpart A—General Provisions

§ 164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation standards under part C of title XI of the Act and section 264 of Public Law 104–191.

§ 164.104 Applicability.

Except as otherwise provided, the provisions of this part apply to covered entities: health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction referred to in section 1173(a)(1) of the Act.

Subpart B–D—[Reserved]

Subpart E—Privacy of Individually Identifiable Health Information

§ 164.502 Applicability.

In addition to the applicable provisions of part 160 of this subchapter and except as otherwise herein provided, the requirements, standards, and implementation specifications of this subpart apply to covered entities with respect to protected health information.

§ 164.504 Definitions.

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

Business partner means, with respect to a covered entity, a person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. ''Business partner'' includes contractors or other persons who receive protected health information from the covered entity (or from another business partner of the covered entity) for the purposes described in the previous sentence, including lawyers, auditors, consultants, third-party administrators, health care clearinghouses, data processing firms, billing firms, and other covered entities. ''Business partner'' excludes persons who are within the covered entity's workforce, as defined in this section.

Designated record set means a group of records under the control of a covered entity from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual and which is used by the covered entity to make decisions about the individual. For purposes of this paragraph, the term *record* means any item, collection, or grouping of protected health information maintained, collected, used, or disseminated by a covered entity.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Health care operations means the following activities undertaken by or on behalf of a covered entity that is a health plan or health care provider for the purpose of carrying out the management functions of such entity necessary for the support of treatment or payment:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines;

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

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

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

(5) Compiling and analyzing information in anticipation of or for use in a civil or criminal legal proceeding.

Health oversight agency means an agency, person or entity, including the employees or agents thereof,

(1) That is:

(i) A public agency; or

(ii) A person or entity acting under grant of authority from or contract with a public agency; and

(2) Which performs or oversees the performance of any audit; investigation; inspection; licensure or discipline; civil, criminal, or administrative proceeding or action; or other activity necessary for appropriate oversight of the health care system, of government benefit programs for which health information is relevant to beneficiary eligibility, or of government regulatory programs for which health information is necessary

for determining compliance with program standards.

Individual means the person who is the subject of protected health information, except that:

(1) ''Individual'' includes:

(i) With respect to adults and emancipated minors, legal representatives (such as court-appointed guardians or persons with a power of attorney), to the extent to which applicable law permits such legal representatives to exercise the person's rights in such contexts.

(ii) With respect to unemancipated minors, a parent, guardian, or person acting *in loco parentis*, provided that when a minor lawfully obtains a health care service without the consent of or notification to a parent, guardian, or other person acting *in loco parentis*, the minor shall have the exclusive right to exercise the rights of an individual under this subpart with respect to the protected health information relating to such care.

(iii) With respect to deceased persons, an executor, administrator, or other person authorized under applicable law to act on behalf of the decedent's estate.

(2) ''Individual'' excludes:

(i) Foreign military and diplomatic personnel and their dependents who receive health care provided by or paid for by the Department of Defense or other federal agency, or by an entity acting on its behalf, pursuant to a country-to-country agreement or federal statute; and

(ii) Overseas foreign national beneficiaries of health care provided by the Department of Defense or other federal agency, or by a non-governmental organization acting on its behalf.

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

(1) Is created by or received from a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and

(i) Which identifies the individual, or

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

Law enforcement official means an officer of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to conduct:

(1) An investigation or official proceeding inquiring into a violation of, or failure to comply with, any law; or

(2) A criminal, civil, or administrative proceeding arising from a violation of, or failure to comply with, any law.

Payment means:

(1) The activities undertaken by or on behalf of a covered entity that is:

(i) A health plan, or by a business partner on behalf of a health plan, to obtain premiums or to determine or fulfill its responsibility for coverage under the health plan and for provision of benefits under the health plan; or

(ii) A health care provider or health plan, or a business partner on behalf of such provider or plan, to obtain reimbursement for the provision of health care.

(2) Activities that constitute payment include:

(i) Determinations of coverage, improving methods of paying or coverage policies, adjudication or subrogation of health benefit claims;

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

(iii) Billing, claims management, and medical data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and

(v) Utilization review activities, including precertification and preauthorization of services.

Protected health information means individually identifiable health information that is or has been electronically transmitted or electronically maintained by a covered entity and includes such information in any other form.

(1) For purposes of this definition,

(i) ''Electronically transmitted'' includes information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmissions over the Internet, Extranet, leased lines, dial-up lines, private networks, telephone voice response, and ''faxback'' systems.

(ii) ''Electronically maintained'' means information stored by a computer or on any electronic medium from which information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

(2) ''Protected health information'' excludes:

(i) Individually identifiable health information in education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and

(ii) Individually identifiable health information of inmates of correctional facilities and detainees in detention facilities.

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

Research means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. ''Generalizable knowledge'' is knowledge related to health that can be applied to populations outside of the population served by the covered entity.

Treatment means the provision of health care by, or the coordination of health care (including health care management of the individual through risk assessment, case management, and disease management) among, health care providers; the referral of a patient from one provider to another; or the coordination of health care or other services among health care providers and third parties authorized by the health plan or the individual.

Use means the employment, application, utilization, examination, or analysis of information within an entity that holds the information.

Workforce means employees, volunteers, trainees, and other persons under the direct control of a covered entity, including persons providing labor on an unpaid basis.

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

(a) *Standard.* A covered entity may not use or disclose an individual's protected health information, except as otherwise permitted or required by this part or as required to comply with applicable requirements of this subchapter.

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

(i) Except for research information unrelated to treatment, to carry out treatment, payment, or health care operations;

(ii) Pursuant to an authorization by the individual that complies with § 164.508; or

(iii) As permitted by and in compliance with this section or § 164.510.

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

(i) To an individual, when a request is made under § 164.514; or

(ii) When required by the Secretary under § 164.522 to investigate or determine the entity's compliance with this part.

(b)(1) *Standard: Minimum necessary.* A covered entity must make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose of the use or disclosure. This requirement does not apply to uses or disclosures that are:

(i) Made in accordance with §§ 164.508(a)(1), 164.514, or § 164.522;

(ii) Required by law and permitted under § 164.510;

(iii) Required for compliance with applicable requirements of this subchapter; or

(iv) Made by a covered health care provider to a covered health plan, when the information is requested for audit and related purposes.

(2) *Implementation specification: Procedures.* To comply with the standard in this paragraph, a covered entity must have procedures to:

(i) Identify appropriate persons within the entity to determine what information should be used or disclosed consistent with the minimum necessary standard;

(ii) Ensure that the persons identified under paragraph (b)(2)(i) of this section make the minimum necessary determinations, when required;

(iii) Within the limits of the entity's technological capabilities, provide for the making of such determinations individually.

(3) *Implementation specification: Reliance.* When making disclosures to public officials that are permitted under § 164.510 but not required by other law, a covered entity may reasonably rely on the representations of such officials that the information requested is the minimum necessary for the stated purpose(s).

(c)(1) *Standard: Right of an individual to restrict uses and disclosures.* (i) A covered entity that is a health care provider must permit individuals to request that uses or disclosures of protected health information for treatment, payment, or health care operations be restricted, and, if the requested restrictions are agreed to by the provider, not make uses or disclosures inconsistent with such restrictions.

(ii) This requirement does not apply:

(A) To uses or disclosures permitted under § 164.510;

(B) When the health care services provided are emergency services or the information is requested pursuant to § 164.510(k) and

(C) To disclosures to the Secretary pursuant to § 164.522.

(iii) A provider is not required to agree to a requested restriction.

(2) *Implementation specifications.* A covered entity must have procedures that:

(i) Provide individuals an opportunity to request a restriction on the uses and disclosures of their protected health information;

(ii) Provide that restrictions that are agreed to by the entity are reduced to writing or otherwise documented;

(iii) Enable the entity to honor such restrictions; and

(iv) Provide for the notification of others to whom such information is disclosed of such restriction.

(d)(1) *Standard: use or disclosure of de-identified protected health information.* The requirements of this subpart do not apply to protected health information that a covered entity has de-identified, provided, however, that:

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

(ii) If a covered entity re-identifies de-identified information, it may use or disclose such re-identified information only in accordance with this subpart.

(2) *Implementation specifications.* (i) A covered entity may use protected health information to create de-identified information by removing, coding, encrypting, or otherwise eliminating or concealing the information that makes such information individually identifiable.

(ii) Information is presumed not to be individually identifiable (de-identified), if:

(A) The following identifiers have been removed or otherwise concealed:

(*1*) Name;

(*2*) Address, including street address, city, county, zip code, and equivalent geocodes;

(*3*) Names of relatives;

(*4*) Name of employers;

(*5*) Birth date;

(*6*) Telephone numbers;

(*7*) Fax numbers;

(*8*) Electronic mail addresses;

(*9*) Social security number;

(*10*) Medical record number;

(*11*) Health plan beneficiary number;

(*12*) Account number;

(*13*) Certificate/license number;

(*14*) Any vehicle or other device serial number;

(*15*) Web Universal Resource Locator (URL);

(*16*) Internet Protocol (IP) address number;

(*17*) Finger or voice prints;

(*18*) Photographic images; and

(*19*) Any other unique identifying number, characteristic, or code that the covered entity has reason to believe may be available to an anticipated recipient of the information; and

(B) The covered entity has no reason to believe that any anticipated recipient of such information could use the information, alone or in combination with other information, to identify an individual.

(iii) Notwithstanding paragraph (d)(2)(ii) of this section, entities with appropriate statistical experience and expertise may treat information as de-identified, if they include information listed in paragraph (d)(2)(ii) of this section and they determine that the probability of identifying individuals with such identifying information retained is very low, or may remove additional information, if they have a reasonable basis to believe such additional information could be used to identify an individual.

(e)(1) *Standards: Business partners.* (i) Except for disclosures of protected health information by a covered entity that is a health care provider to another health care provider for consultation or referral purposes, a covered entity may not disclose protected health information to a business partner without satisfactory assurance from the business partner that it will appropriately safeguard the information.

(ii) A covered entity must take reasonable steps to ensure that each business partner complies with the requirements of this subpart with respect to any task or other activity it performs on behalf of the entity, to the extent the covered entity would be required to comply with such requirements.

(2) *Implementation specifications.* (i) For the purposes of this section, *satisfactory assurance* means a contract between the covered entity and the business partner to which such information is to be disclosed that establishes the permitted and required uses and disclosures of such information by the partner. The contract must provide that the business partner will:

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

(B) Not use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;

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

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

(E) Ensure that any subcontractors or agents to whom it provides protected health information received from the covered entity agree to the same restrictions and conditions that apply to the business partner with respect to such information;

(F) Make available protected health information in accordance with § 164.514(a);

(G) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart;

(H) At termination of the contract, return or destroy all protected health information received from the covered entity that the business partner still maintains in any form and retain no copies of such information; and

(I) Incorporate any amendments or corrections to protected health information when notified pursuant to § 164.516(c)(3).

(ii) The contract required by paragraph (e)(2)(i) of this section must:

(A) State that the individuals whose protected health information is disclosed under the contract are intended third party beneficiaries of the contract; and

(B) Authorize the covered entity to terminate the contract, if the covered entity determines that the business partner has violated a material term of the contract required by this paragraph.

(iii) A material breach by a business partner of its obligations under the contract required by paragraph (e)(2)(i) of this section will be considered to be noncompliance of the covered entity with the applicable requirements of this subpart, if the covered entity knew or reasonably should have known of such breach and failed to take reasonable steps to cure the breach or terminate the contract.

(f) *Standard: Deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for two years following the death of such individual. This requirement does not apply to uses or disclosures for research purposes.

(g) *Standard: uses and disclosures consistent with notice.* Except as provided by § 164.520(g)(2), a covered entity that is required by § 164.512 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice.

§ 164.508 Uses and disclosures for which individual authorization is required.

(a) *Standard.* An authorization executed in accordance with this section is required in order for the covered entity to use or disclose protected health information in the following situations:

(1) *Request by individual.* Where the individual requests the covered entity to use or disclose the information.

(2) *Request by covered entity.* (i) Where the covered entity requests the individual to authorize the use or disclosure of the information. The covered entity must request and obtain an authorization from the individual for all uses and disclosures that are not:

(A) Except as provided in paragraph (a)(3) of this section, compatible with or directly related to treatment, payment, or health care operations;

(B) Covered by § 164.510;

(C) Covered by paragraph (a)(1) of this section; or

(D) Required by this subpart.

(ii) Uses and disclosures of protected health information for which individual authorization is required include, but are not limited to, the following:

(A) Use for marketing of health and non-health items and services by the covered entity;

(B) Disclosure by sale, rental, or barter;

(C) Use and disclosure to non-health related divisions of the covered entity, e.g., for use in marketing life or casualty insurance or banking services;

(D) Disclosure, prior to an individual's enrollment in a health plan, to the health plan or health care provider for making eligibility or enrollment determinations relating to the individual or for underwriting or risk rating determinations;

(E) Disclosure to an employer for use in employment determinations; and

(F) Use or disclosure for fundraising purposes.

(iii) A covered entity may not condition the provision to an individual of treatment or payment on the provision by the individual of a requested authorization for use or disclosure, except where the authorization is requested in connection with a clinical trial.

(iv) Except where required by law, a covered entity may not require an individual to sign an authorization for use or disclosure of protected health information for treatment, payment, or health care operations purposes.

(3) *Authorization required: Special cases.* (i) Except as otherwise required by this subpart or permitted under § 164.510, a covered entity must obtain the authorization of the individual for the following uses and disclosures of protected health information about the individual:

(A) Use by a person other than the creator, or disclosure, of psychotherapy notes; and

(B) Use or disclosure of research information unrelated to treatment.

(ii) The requirements of paragraphs (b) through (e) of this section apply to such authorizations, as appropriate.

(iii) A covered entity may not condition treatment, enrollment in a health plan, or payment on a requirement that the individual authorize use or disclosure of psychotherapy notes relating to the individual.

(iv) For purposes of this section:

(A) *Psychotherapy notes* means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session. For purposes of this definition, ''psychotherapy notes'' excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis and progress to date.

(B) *Research information unrelated to treatment* means health information that is received or created by a covered entity in the course of conducting research, for which there is insufficient scientific and medical evidence regarding the validity or utility of the information such that it should not be used for the purpose of providing health care, and with respect to which the covered entity has not requested payment from a third party payor.

(b) *General implementation specifications for authorizations.*—(1) *General requirements.* A copy of the model form which appears in Appendix A hereto, or a document that contains the elements listed in paragraphs (c) or (d) of this section, as applicable, must be accepted by the covered entity.

(2) *Defective authorizations.* There is no ''authorization'' within the meaning of this section, if the submitted form has any of the following defects:

(i) The expiration date has passed;

(ii) The form has not been filled out completely;

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The form lacks an element required by paragraph (c) or (d) of this section, as applicable;

(v) The information on the form is known by the covered entity to be false.

(3) *Compound authorizations.* Except where authorization is requested in connection with a clinical trial, an authorization for use or disclosure of protected health information for purposes other than treatment or payment may not be in the same document as an authorization for or consent to treatment or payment.

(c) *Implementation specifications for authorizations requested by an individual.*—(1) *Required elements.* Before a covered entity may use or disclose protected health information of an individual pursuant to a request from the individual, it must obtain a completed authorization for use or disclosure executed by the individual that contains at least the following elements:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

(ii) The name of the covered entity, or class of entities or persons, authorized to make the requested use or disclosure;

(iii) The name or other specific identification of the person(s) or entity(ies), which may include the covered entity itself, to whom the covered entity may make the requested use or disclosure;

(iv) An expiration date;

(v) Signature and date;

(vi) If the authorization is executed by a legal representative or other person authorized to act for the individual, a description of his or her authority to act or relationship to the individual;

(vii) A statement in which the individual acknowledges that he or she has the right to revoke the authorization, except to the extent that information has already been released under the authorization; and

(viii) A statement in which the individual acknowledges that information used or disclosed to any entity other than a health plan or health care provider may no longer be protected by the federal privacy law.

(2) *Plain language requirement.* The model form at appendix A to this subpart may be used. If the model form at appendix A to this subpart is not used, the authorization form must be written in plain language.

(d) *Implementation specifications for authorizations for uses and disclosures requested by covered entities.*—(1) *Required elements.* Before a covered entity may use or disclose protected health information of an individual pursuant to a request that it has made, it must obtain a completed authorization for use or disclosure executed by the individual that meets the requirements of paragraph (c) of this section and contains the following additional elements:

(i) Except where the authorization is requested for a clinical trial, a statement that it will not condition treatment or payment on the individual's providing authorization for the requested use or disclosure;

(ii) A description of the purpose(s) of the requested use or disclosure;

(iii) A statement that the individual may:

(A) Inspect or copy the protected health information to be used or disclosed as provided in § 164.514; and

(B) Refuse to sign the authorization; and

(iv) Where use or disclosure of the requested information will result in financial gain to the entity, a statement that such gain will result.

(2) *Required procedures.* In requesting authorization from an individual under this paragraph, a covered entity must:

(i) Have procedures designed to enable it to request only the minimum amount of protected health information necessary to accomplish the purpose for which the request is made; and

(ii) Provide the individual with a copy of the executed authorization.

(e) *Revocation of authorizations.* An individual may revoke an authorization to use or disclose his or her protected health information at any time, except to the extent that the covered entity has taken action in reliance thereon.

§ 164.510 Uses and disclosures for which individual authorization is not required.

A covered entity may use or disclose protected health information, for purposes other than treatment, payment, or health care operations, without the authorization of the individual, in the situations covered by this section and subject to the applicable requirements provided for by this section.

(a) *General requirements.* In using or disclosing protected health information under this section:

(1) *Verification.* A covered entity must comply with any applicable verification requirements under § 164.518(c).

(2) *Health care clearinghouses.* A health care clearinghouse that uses or discloses protected health information it maintains as a business partner of a covered entity may not make uses or disclosures otherwise permitted under this section that are not permitted by the terms of its contract with the covered entity under § 164.506(e).

(b) *Disclosures and uses for public health activities.*—(1) *Permitted disclosures.* A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions;

(ii) A public health authority or other appropriate authority authorized by law to receive reports of child abuse or neglect;

(iii) A person or entity other than a governmental authority that can demonstrate or demonstrates that it is acting to comply with requirements or direction of a public health authority; or

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition and is authorized by law to be notified as necessary in the conduct of a public health intervention or investigation.

(2) *Permitted use.* Where the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) *Disclosures and uses for health oversight activities.*—(1) *Permitted disclosures.* A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audit, investigation, inspection, civil, criminal, or administrative proceeding or action, or other activity necessary for appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility; or

(iii) Government regulatory programs for which health information is necessary for determining compliance with program standards.

(2) *Permitted use.* Where a covered entity is itself a health oversight agency, the covered entity may use protected health information for health oversight activities described by paragraph (c)(1) of this section.

(d) *Disclosures and uses for judicial and administrative proceedings.*—(1) *Permitted disclosures.* A covered entity may disclose protected health

information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal; or

(ii) Where the individual is a party to the proceeding and his or her medical condition or history is at issue and the disclosure is pursuant to lawful process or otherwise authorized by law.

(2) *Permitted use.* Where the covered entity is itself a government agency, the covered entity may use protected health information in all cases in which it is permitted to disclose such information in the course of any judicial or administrative proceeding under paragraph (d)(1) of this section.

(3) *Additional restriction.* (i) Where the request for disclosure of protected health information is accompanied by a court order, the covered entity may disclose only that protected health information which the court order authorizes to be disclosed.

(ii) Where the request for disclosure of protected health information is not accompanied by a court order, the covered entity may not disclose the information requested unless a request authorized by law has been made by the agency requesting the information or by legal counsel representing a party to litigation, with a written statement certifying that the protected health information requested concerns a litigant to the proceeding and that the health condition of such litigant is at issue at such proceeding.

(e) *Disclosures to coroners and medical examiners.* A covered entity may disclose protected health information to a coroner or medical examiner, consistent with applicable law, for the purposes of identifying a deceased person or determining a cause of death.

(f) *Disclosures for law enforcement purposes.* A covered entity may disclose protected health information to a law enforcement official if:

(1) *Pursuant to process.* (i) The law enforcement official is conducting or supervising a law enforcement inquiry or proceeding authorized by law and the disclosure is:

(A) Pursuant to a warrant, subpoena, or order issued by a judicial officer that documents a finding by the judicial officer;

(B) Pursuant to a grand jury subpoena; or

(C) Pursuant to an administrative request, including an administrative subpoena or summons, a civil investigative demand, or similar process authorized under law, provided that:

(*1*) The information sought is relevant and material to a legitimate law enforcement inquiry;

(*2*) The request is as specific and narrowly drawn as is reasonably practicable; and

(*3*) De-identified information could not reasonably be used.

(ii) For the purposes of this paragraph, ''law enforcement inquiry or proceeding'' means:

(A) An investigation or official proceeding inquiring into a violation of, or failure to comply with, law; or

(B) A criminal, civil, or administrative proceeding arising from a violation of, or failure to comply with, law.

(2) *Limited information for identifying purposes.* The disclosure is for the purpose of identifying a suspect, fugitive, material witness, or missing person, *provided* that, the covered entity may disclose only the following information:

(i) Name;

(ii) Address;

(iii) Social security number;

(iv) Date of birth;

(v) Place of birth;

(vi) Type of injury or other distinguishing characteristic; and

(vii) Date and time of treatment.

(3) *Information about a victim of crime or abuse.* The disclosure is of the protected health information of an individual who is or is suspected to be a victim of a crime, abuse, or other harm, if the law enforcement official represents that:

(i) Such information is needed to determine whether a violation of law by a person other than the victim has occurred; and

(ii) Immediate law enforcement activity that depends upon obtaining such information may be necessary.

(4) *Intelligence and national security activities.* The disclosure is:

(i) For the conduct of lawful intelligence activities conducted pursuant to the National Security Act (50 U.S.C. 401, *et seq.*);

(ii) Made in connection with providing protective services to the President or other persons pursuant to 18 U.S.C. 3056; or

(iii) Made pursuant to 22 U.S.C. 2709(a)(3).

(5) *Health care fraud.* The covered entity believes in good faith that the information disclosed constitutes evidence of criminal conduct:

(i) That arises out of and is directly related to:

(A) The receipt of health care or payment for health care, including a fraudulent claim for health care;

(B) Qualification for or receipt of benefits, payments, or services based on a fraudulent statement or material misrepresentation of the health of the individual;

(ii) That occurred on the premises of the covered entity; or

(iii) Was witnessed by a member of the covered entity's workforce.

(5) *Urgent circumstances.* The disclosure is of the protected health information of an individual who is or is suspected to be a victim of a crime, abuse, or other harm, if the law enforcement official represents that:

(i) Such information is needed to determine whether a violation of law by a person other than the victim has occurred; and

(ii) Immediate law enforcement activity that depends upon obtaining such information may be necessary.

(g) *Disclosures and uses for governmental health data systems.*—(1) *Permitted disclosures.* A covered entity may disclose protected health information to a government agency, or private entity acting on behalf of a government agency, for inclusion in a governmental health data system that collects health data for analysis in support of policy, planning, regulatory, or management functions authorized by law.

(2) *Permitted uses.* Where a covered entity is itself a government agency that collects health data for analysis in support of policy, planning, regulatory, or management functions, the covered entity may use protected health information in all cases in which it is permitted to disclose such information for government health data systems under paragraph (g)(1) of this section.

(h) *Disclosures of directory information.* (1) *Individuals with capacity.* For individuals with the capacity to make their own health care decisions, a covered entity that is a health care provider may disclose protected health information for directory purposes, provided that, the individual has agreed to such disclosure.

(2) *Incapacitated individuals.* For individuals who are incapacitated, a covered entity that is a health care provider may, at its discretion and consistent with good medical practice and any prior expressions of preference of which the covered entity is aware, disclose protected health information for directory purposes.

(3) *Information to be disclosed.* The information that may be disclosed for directory purposes pursuant to paragraphs (h)(1) and (2) of this section, is limited to:

(i) Name of the individual;

(ii) Location of the individual in the health care provider's facility; and

(iii) Description of the individual's condition in general terms that do not

communicate specific medical information about the individual.

(i) *Disclosures for banking and payment processes.* A covered entity may disclose, in connection with routine banking activities or payment by debit, credit, or other payment card, or other payment means, the minimum amount of protected health information necessary to complete a banking or payment activity to:

(1) *Financial institutions.* An entity engaged in the activities of a financial institution (as defined in section 1101 of the Right to Financial Privacy Act of 1978); or

(2) *Entities acting on behalf of financial institutions.* An entity engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for an entity described in paragraph (i)(1) of this section.

(j) *Uses and disclosures for research purposes.* A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that, the covered entity has obtained written documentation of the following:

(1) *Waiver of authorization.* A waiver, in whole or in part, of authorization for use or disclosure of protected health information that has been approved by either:

(i) An Institutional Review Board, established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 28 CFR 46.107.32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107.45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(ii) A privacy board that:

(A) Has members with varying backgrounds and appropriate professional competency as necessary to review the research protocol;

(B) Includes at least one member who is not affiliated with the entity conducting the research or related to a person who is affiliated with such entity; and

(C) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(2) *Date of approval.* The date of approval of the waiver, in whole or in part, of authorization by an Institutional Review Board or privacy board.

(3) *Criteria.* The Institutional Review Board or privacy board has determined that the waiver, in whole or in part, of authorization satisfies the following criteria:

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

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

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

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

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

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

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

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

(4) *Required signature.* The written documentation must be signed by the chair of, as applicable, the Institutional Review Board or the privacy board.

(k) *Uses and disclosures in emergency circumstances.*—(1) *Permitted disclosures.* A covered entity may, consistent with applicable law and standards of ethical conduct and based on a reasonable belief that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, use or disclose protected health information to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

(2) *Presumption of reasonable belief.* A covered entity that makes a disclosure pursuant to paragraph (k)(1) of this section is presumed to have acted under a reasonable belief, if the disclosure is made in good faith based upon a credible representation by a person with apparent knowledge or authority (such as a doctor or law enforcement or other government official).

(l) *Disclosures to next-of-kin.*—(1) *Permitted disclosures.* A covered entity may disclose protected health information to a person who is a next-of-kin, other family member, or close personal friend of an individual who possesses the capacity to make his or her own health care decisions, if:

(i) The individual has verbally agreed to the disclosure; or

(ii) In circumstances where such agreement cannot practicably or reasonably be obtained, only the protected health information that is directly relevant to the person's involvement in the individual's health care is disclosed, consistent with good health professional practices and ethics.

(2) *Next-of-kin defined.* For purposes of this paragraph, ''next-of-kin'' is defined as defined under applicable law.

(m) *Uses and disclosures for specialized classes.*—(1) *Military purposes.* A covered entity that is a health care provider or health plan providing health care to individuals who are Armed Forces personnel may use and disclose protected health information for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, where the appropriate military authority has published by notice in the **Federal Register** the following information:

(i) Appropriate military command authorities;

(ii) The circumstances for which use or disclosure without individual authorization would be required; and

(iii) Activities for which such use or disclosure would occur in order to assure proper execution of the military mission.

(2) *Department of Veterans Affairs.* The Department of Veterans Affairs may use and disclose protected health information among components of the Department that determine eligibility for or entitlement to, or that provide, benefits under laws administered by the Secretary of Veterans Affairs.

(3) *Intelligence community.* A covered entity may disclose protected health information of an individual who is an employee of the intelligence community, as defined in section 4 of the National Security Act, 50 U.S.C. 401a, and his or her dependents, if such dependents are being considered for posting abroad, to intelligence community agencies, where authorized by law.

(4) *Department of State.* The Department of State may use protected health information about the following individuals for the following purposes:

(i) As to applicants to the Foreign Service, for medical clearance determinations about physical fitness to serve in the Foreign Service on a worldwide basis, including about medical and mental conditions limiting assignability abroad; determinations of conformance to occupational physical standards, where applicable; and determinations of suitability.

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

(iii) As to eligible family members of Foreign Service or other United States Government employees, for medical clearance determinations as described in paragraph (m)(4)(ii) of this section to permit eligible family members to accompany employees to posts abroad on Government orders; determinations regarding family members remaining at post; and separation medical examinations.

(n) *Uses and disclosures otherwise required by law.* A covered entity may use or disclose protected health information where such use or disclosure is required by law and the use or disclosure meets all relevant requirements of such law. This paragraph does not apply to uses or disclosures that are covered by paragraphs (b) through (m) of this section.

§ 164.512 Notice to individuals of information practices.

(a) *Standard.* An individual has a right to adequate notice of the policies and procedures of a covered entity that is a health plan or a health care provider with respect to protected health information.

(b) *Standard for notice procedures.* A covered entity that is a health plan or health care provider must have procedures that provide adequate notice to individuals of their rights and the procedures for exercising their rights under this subpart with respect to protected health information about them.

(c) *General implementation specification.* A covered entity that has and follows procedures that meet the requirements of this section will be presumed to have provided adequate notice under this section.

(d) *Implementation specifications: content of notice.*—(1) *Required elements.* Notices required to be provided under this section must include in plain language a statement of each of the following elements:

(i) *Uses and disclosures.* The uses and disclosures, and the entity's policies and procedures with respect to such uses and disclosures, must be described in sufficient detail to put the individual on notice of the uses and disclosures expected to be made of his or her protected health information. Such statement must:

(A) Describe the uses and disclosures that will be made without individual authorization; and

(B) Distinguish between those uses and disclosures the entity makes that are required by law and those that are permitted but not required by law.

(ii) *Required statements.* State that:

(A) Other uses and disclosures will be made only with the individual's authorization and that such authorization may be revoked;

(B) An individual may request that certain uses and disclosures of his or her protected health information be restricted, and the covered entity is not required to agree to such a request;

(C) An individual has the right to request, and a description of the procedures for exercising, the following with respect to his or her protected health information:

(*1*) Inspection and copying;

(*2*) Amendment or correction; and

(*3*) An accounting of the disclosures of such information by the covered entity;

(D) The covered entity is required by law to protect the privacy of its individually identifiable health information, provide a notice of its policies and procedures with respect to such information, and abide by the terms of the notice currently in effect;

(E) The entity may change its policies and procedures relating to protected health information at any time, with a description of how individuals will be informed of material changes; and

(F) Individuals may complain to the covered entity and to the Secretary if they believe that their privacy rights have been violated.

(iii) *Contact.* The name and telephone number of a contact person or office required by § 164.518(a)(2).

(iv) *Date.* The date the version of the notice was produced.

(2) *Revisions.* A covered health plan or health care provider may change its policies or procedures required by this subpart at any time. When a covered health plan or health care provider materially revises its policies and procedures, it must update its notice as provided for by § 164.520(g).

(e) *Implementation specifications: Provision of notice.* A covered entity must make the notice required by this section available:

(1) *General requirement.* On request; and

(2) *Specific requirements.* As follows:

(i) *Health plans.* Health plans must provide a copy of the notice to an individual covered by the plan:

(A) As of the date on which the health plan is required to be in compliance with this subpart;

(B) After the date described in paragraph (e)(2)(i)(A) of this section, at enrollment;

(C) After enrollment, within 60 days of a material revision to the content of the notice; and

(D) No less frequently than once every three years.

(ii) *Health care providers.* A health care provider must:

(A) During the one year period following the date by which the provider is required to come into compliance with this subpart, provide a copy to individuals currently served by the provider at the first service delivery to such individuals during such period, provided that, where service is not provided through a face-to-face contact, the provider must provide the notice in an appropriate manner within a reasonable period of time following first service delivery;

(B) After the one year period provided for by paragraph (e)(2)(ii)(A) of this section, provide a copy to individuals served by the provider at the first service delivery to such individuals, provided that, where service is not provided through a face-to-face contact, the provider must provide the notice in an appropriate manner within a reasonable period of time following first service delivery; and

(C) Post a copy of the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the provider to be able to read the notice. Any revision to the notice must be posted promptly.

§ 164.514 Access of individuals to protected health information

(a) *Standard: Right of access.* An individual has a right of access to, which includes a right to inspect and obtain a copy of, his or her protected health information in designated record sets of a covered entity that is a health plan or a health care provider, including such information in a business partner's designated record set that is not a duplicate of the information held by the provider or plan, for so long as the information is maintained.

(b) *Standard: denial of access to protected health information.*—(1) *Grounds.* Except where the protected

health information to which access is requested is subject to 5 U.S.C. 552a, a covered entity may deny a request for access under paragraph (a) of this section where:

(i) A licensed health care professional has determined that, in the exercise of reasonable professional judgment, the inspection and copying requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The information is about another person (other than a health care provider) and a licensed health care professional has determined that the inspection and copying requested is reasonably likely to cause substantial harm to such other person;

(iii) The information was obtained under a promise of confidentiality from someone other than a health care provider and such access would be likely to reveal the source of the information;

(iv) The information was obtained by a covered entity that is a health care provider in the course of a clinical trial, the individual has agreed to the denial of access when consenting to participate in the trial (if the individual's consent to participate was obtained), and the clinical trial is in progress; or

(v) The information was compiled in reasonable anticipation of, or for use in, a legal proceeding.

(2) *Other information available.* Where a denial of protected health information is made pursuant to paragraph (b)(1) of this section, the covered entity must make any other protected health information requested available to the individual to the extent possible consistent with the denial.

(c) *Standard: procedures to protect rights of access.* A covered entity that is a health plan or a health care provider must have procedures that enable individuals to exercise their rights under paragraph (a) of this section.

(d) *Implementation specifications: Access to protected health information.* The procedures required by paragraph (c) of this section must:

(1) *Means of request.* Provide a means by which an individual can request inspection or a copy of protected health information about him or her.

(2) *Time limit.* Provide for taking action on such requests as soon as possible but not later than 30 days following receipt of the request.

(3) *Request accepted.* Where the request is accepted, provide:

(i) For notification of the individual of the decision and of any steps necessary to fulfill the request;

(ii) The information requested in the form or format requested, if it is readily producible in such form or format;

(iii) For facilitating the process of inspection and copying; and

(iv) For a reasonable, cost-based fee for copying health information provided pursuant to this paragraph, if deemed desirable by the entity.

(4) *Request denied.* Where the request is denied in whole or in part, provide the individual with a written statement in plain language of:

(i) The basis for the denial; and

(ii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.518(d)(2) or to the Secretary pursuant to the procedures established in § 164.522(b). The description must include:

(A) The name and telephone number of the contact person or office required by § 164.518(a)(2) of this subpart; and

(B) Information relevant to filing a complaint with the Secretary under § 164.522(b).

§ 164.515 Accounting for disclosures of protected health information.

(a) *Standard: Right to an accounting of disclosures of protected health information.* An individual has a right to receive an accounting of all disclosures of protected health information made by a covered entity as long as such information is maintained by the entity, except for disclosures:

(1) For treatment, payment and health care operations; and

(2) To health oversight or law enforcement agencies, if the health oversight or law enforcement agency has provided a written request stating that the exclusion is necessary because disclosure would be reasonably likely to impede the agency's activities and specifying the time for which such exclusion is required.

(b) *Standard: Procedures for accounting.* A covered entity must have procedures to give individuals an accurate accounting of disclosures for which an accounting is required by paragraph (a) of this section.

(c) *Implementation specifications: Accounting procedures.* The procedures required by paragraph (b) of this section must:

(1) Provide for an accounting of the following:

(i) The date of each disclosure;

(ii) The name and address of the organization or person who received the protected health information;

(iii) A brief description of the information disclosed;

(iv) For disclosures other than those made at the request of the individual, the purpose for which the information was disclosed; and (v) Provision of copies of all requests for disclosure.

(2) Provide the accounting to the individual as soon as possible, but no later than 30 days of receipt of the request therefor.

(3) Provide for a means of accounting for as long as the entity maintains the protected health information.

(4) Provide for a means of requiring business partners to provide such an accounting upon request of the covered entity.

§ 164.516 Amendment and correction.

(a) *Standard: right to request amendment or correction.*—(1) *Right to request.* An individual has the right to request a covered entity that is a health plan or health care provider to amend or correct protected health information about him or her in designated record sets of the covered entity for as long as the covered entity maintains the information.

(2) *Grounds for denial of request.* A covered entity may deny a request for amendment or correction of the individual's protected health information, if it determines that the information that is the subject of the request:

(i) Was not created by the covered entity;

(ii) Would not be available for inspection and copying under § 164.514 or

(iii) Is accurate and complete.

(b) *Standard: Amendment and correction procedures.* A covered entity that is a health plan or health care provider must have procedures to enable individuals to request amendment or correction, to determine whether the requests should be granted or denied, and to disseminate amendments or corrections to its business partners and others to whom erroneous information has been disclosed.

(c) *Implementation specifications: Procedures.* The procedures required by paragraph (b) of this section must provide that the covered entity will:

(1) *Means of request.* Provide a means by which an individual can request amendment or correction of his or her protected health information.

(2) *Time limit.* Take action on such request within 60 days of receipt of the request;

(3) *Request accepted.* Where the request is accepted in whole or in part:

(i) As otherwise required by this part, make the appropriate amendments or corrections;

(ii) As otherwise required by this part, identify the challenged entries as

amended or corrected and indicate their location;

(iii) Make reasonable efforts to notify:

(A) Persons, organizations, or other entities the individual identifies as needing to be notified; and (B) Persons, organizations, or other entities, including business partners, who the covered entity knows have received the erroneous or incomplete information and who may have relied, or could foreseeably rely, on such information to the detriment of the individual; and (iv) Notify the individual of the decision to correct or amend the information.

(4) *Request denied.* Where the request is denied in whole or in part:

(i) Provide the individual with a written statement in plain language of:

(A) The basis for the denial;

(B) A description of how the individual may file a written statement of disagreement with the denial; and

(C) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.518(d) or to the Secretary pursuant to the procedures established in § 164.522(b). The description must include:

(*1*) The name and telephone number of the contact person or office required by § 164.518(a)(2); and

(*2*) Information relevant to filing a complaint with the Secretary under § 164.522(b).

(ii) The procedures of the covered entity must:

(A) Permit the individual to file a statement of the individual's disagreement with the denial and the basis of such disagreement.

(B) Provide for inclusion of the covered entity's statement of denial and the individual's statement of disagreement with any subsequent disclosure of the information to which the disagreement relates, provided, however, that the covered entity may establish a limit to the length of the statement of disagreement, and may summarize the statement of disagreement if necessary.

(C) Permit the covered entity to provide a rebuttal to the statement of disagreement in subsequent disclosures under paragraph (c)(4)(ii)(B) of this section.

(d) *Standard: Effectuating a notice of amendment or correction.* Any covered entity that receives a notice of amendment or correction must have procedures in place to make the amendment or correction in any of its designated record sets and to notify its business partners, as appropriate, of necessary amendments or corrections of protected health information.

(e) *Implementation specification: effectuating a notice of amendment or correction.* The procedures required by paragraph (d) of this section must specify the process for correction or amendment of information in all appropriate designated record sets maintained by the covered entity and its business partners.

§ 164.518 Administrative requirements.

Except as otherwise provided, a covered entity must meet the requirements of this section.

(a) *Designated privacy official: standard.*—(1) *Responsibilities of designated privacy official.* A covered entity must designate a privacy official who is responsible for the development and implementation of the privacy policies and procedures of the entity.

(2) *Contact person or office.* A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.512. If a covered entity designates a contact person, it may designate the privacy official as the contact person.

(b) *Training.*—(1) *Standard.* All members of the covered entity's workforce who, by virtue of their positions, are likely to obtain access to protected health information must receive training on the entity's policies and procedures required by this subpart that are relevant to carrying out their function within the entity.

(2) *Implementation specification.* A covered entity must train all members of its workforce who, by virtue of their positions, are likely to obtain access to protected health information. Such training must meet the following requirements:

(i) The training must occur:

(A) For members of the covered entity's workforce as of the date on which this subpart becomes applicable to such entity, by such date; and

(B) For persons joining the covered entity's workforce after the date in paragraph (b)(2)(i)(A) of this section, within a reasonable period after the person joins the workforce.

(ii) The covered entity must require members of its workforce trained as required by this section to sign, upon completing training, a certification. The certification must state:

(A) The date of training; and

(B) That the person completing the training will honor all of the entity's policies and procedures required by this subpart.

(iii) The covered entity must require members of its workforce trained as required by this section to sign, at least once every three years, a statement certifying that the person will honor all of the entity's policies and procedures required by this subpart.

(iv) The covered entity must provide all members of its workforce with access to protected health information within the entity with further training, as relevant to their function within the entity, whenever the entity materially changes its privacy policies or procedures.

(c) *Safeguards.*—(1) *Standard.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2) *Implementation specification: Verification procedures.* A covered entity must have administrative, technical, and physical procedures in place to protect the privacy of protected health information. Such procedures must include adequate procedures for verification of the identity and/or authority, as required by this subpart, of persons requesting such information, where such identity or authority is not known to the entity, as follows:

(i) The covered entity must use procedures that are reasonably likely to establish that the individual or person making the request has the appropriate identity for the use or disclosure requested, except for uses and disclosures that are:

(A) Permitted by this subpart and made on a routine basis to persons or other entities with which the covered entity interacts in the normal course of business or otherwise known to the covered entity; or

(B) Covered by paragraphs (c)(2)(ii), (iii), or (iv) of this section.

(ii) When the request for information is made by a government agency under § 164.510(b), § 164.510(c), § 164.510(e), § 164.510(f), § 164.510(g), § 164.510(m), § 164.510(n), or § 164.522, and the identity and/or authority are not known to the covered entity, the covered entity may not disclose such information without reasonable evidence of identity and/or authority to obtain the information.

(A) For purposes of this paragraph, ''reasonable evidence of identity'' means:

(*1*) A written request on the agency's letterhead;

(*2*) Presentation of an agency identification badge or official credentials; or

(*3*) Similar proof of government status.

(B) For purposes of this paragraph, *reasonable evidence of authority* means:

(*1*) A written statement of the legal authority under which the information is requested; a request for disclosure made by official legal process issued by a grand jury or a judicial or administrative body is presumed to constitute reasonable legal authority; or

(*2*) Where the request is made orally, an oral statement of such authority.

(iii) When the request for information is made by a person or entity acting on behalf of a government agency under § 164.510(b), § 164.510(c), § 164.510(g), or § 164.510(n), and the identity and/or authority are not known to the covered entity, the covered entity may not disclose such information without reasonable evidence of identity and/or authority to obtain the information.

(A) For the purposes of this paragraph, *reasonable evidence of identity* means:

(*1*) A written statement from the government agency, on the agency's letterhead, that the person or entity is acting under the agency's authority; or

(*2*) Other evidence or documentation, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person or entity is acting on behalf of or under the agency's authority.

(B) For the purposes of this paragraph, ''reasonable evidence of authority'' means a statement that complies with paragraph (c)(ii)(B) of this section.

(iv) For uses and disclosures under § 164.510(d), § 164.510(h), or § 164.510(j), compliance with the applicable requirements of those sections constitutes adequate verification under this section.

(v)(A) A covered entity may reasonably rely on evidence of identity and legal authority that meets the requirements of this paragraph.

(B) Where presentation of particular documentation or statements are required by this subpart as a condition of disclosure, a covered entity may reasonably rely on documentation or statements that on their face meet the applicable requirements.

(3) *Implementation specification: Other safeguards.* A covered entity must have safeguards to ensure that information is not used in violation of the requirements of this subpart or by members of its workforce or components of the entity or employees and other persons associated with, or components of, its business partners who are not authorized to access the information.

(4) *Implementation specification: Disclosures by whistleblowers.* A covered entity is not considered to have violated the requirements of this subpart where a member of its workforce or an employee or other person associated with a business partner discloses protected health information that such member or other person believes is evidence of a violation of law to:

(i) The law enforcement official or oversight agency authorized to enforce such law; or

(ii) An attorney, for the purpose of determining whether a violation of law has occurred or assessing what remedies or actions at law may be available to the employee.

(d) *Complaints to the covered entity*—(1) *Standard.* A covered entity that is a health plan or health care provider must provide a process whereby individuals may make complaints concerning the entity's compliance with the requirements established by this subpart.

(2) *Implementation specifications.* A covered entity that is a health plan or health care provider must develop and implement procedures under which an individual may file a complaint alleging that the covered entity failed to comply with one or more requirements of this subpart. Such procedures must provide for:

(i) The identification of the contact person or office required by paragraph (a)(2) of this section; and

(ii) Maintenance by the covered entity of a record of all complaints and their disposition, if any.

(e) *Sanctions: Standard.* A covered entity must develop and apply when appropriate sanctions against members of its workforce who fail to comply with the policies and procedures of the covered entity or the requirements of this subpart in connection with protected health information held by the covered entity or its business partners.

(f) *Duty to mitigate: standard.* A covered entity must have procedures for mitigating, to the extent practicable, any deleterious effect of a use or disclosure of protected health information in violation of this subpart.

§ 164.520 Documentation of policies and procedures.

(a) *Standard.* A covered entity must adequately document its compliance with the applicable requirements of this subpart.

(b) *Implementation specification: General.* A covered entity must document its policies and procedures for complying with the applicable requirements of this subpart. Such documentation must include, but is not limited to, documentation that meets the requirements of paragraphs (c) through (g) of this section.

(c) *Implementation specification: Uses and disclosures.* With respect to uses by the covered entity or its business partners of protected health information, a covered entity must document its policies and procedures regarding:

(1) Uses and disclosures of such information, including:

(i) Uses and disclosures with authorization, including for revocation of authorizations; and

(ii) Uses and disclosures without authorization, including:

(A) For treatment, payment, and health care operations;

(B) For disclosures to business partners, including monitoring and mitigation; and

(C) For uses and disclosures pursuant to § 164.510.

(2) For implementation of the minimum necessary requirement of § 164.506(b).

(3) For implementation of the right to request a restriction under § 164.506(c), including:

(A) Who, if anyone, in the covered entity is authorized to agree to such a request; and

(B) How restrictions agreed to are implemented.

(4) For creation of de-identified information in accordance with § 164.506(d).

(d) *Implementation specification: Individual rights.* A covered entity must document its policies and procedures under §§ 164.512, 164.514, 164.515, and 164.516, as applicable, including:

(1) How notices will be disseminated in accordance with § 164.512;

(2) Designated record sets to which access will be granted under § 164.514;

(3) Grounds for denying requests for access under § 164.514;

(4) Copying fees, if any;

(5) Procedures for providing accounting pursuant to § 164.515;

(6) Procedures for accepting or denying requests for amendment or correction under § 164.516;

(7) How other entities will be notified of amendments or corrections accepted under § 164.516; and

(8) Identification of persons responsible for making decisions or otherwise taking action, including serving as a contact person, under §§ 164.512, 164.514, 164.515, and 164.516.

(e) *Implementation specification: Administrative requirements.* A covered entity must provide documentation of its procedures for complying with § 164.518, including:

(1) Identification of the persons or offices required by § 164.518(a) and their duties;

(2) Training provided as required by § 164.518(b);

(3) How access to protected health information is regulated by the covered entity and its business partners, including safeguards required by § 164.518(c);

(4) For a covered entity that is a health plan or health care provider, for receiving complaints under § 164.518(d);

(5) Sanctions, and the application thereof, required by § 164.518(e); and

(6) Procedures for mitigation under § 164.518(f).

(f) *Implementation specification: Specific documentation required.* A covered entity must retain documentation of the following for six years from when the documentation is created, unless a longer period applies under this subpart:

(1) Restrictions agreed to pursuant to § 164.506(c);

(2) Contracts pursuant to § 164.506(e);

(3) Authorization forms used pursuant to § 164.508;

(4) Samples of all notices issued pursuant to § 164.512;

(5) Written statements required by § 164.514;

(6) The accounting required by § 164.515;

(7) Documents relating to denials of requests for amendment and correction pursuant to § 164.516;

(8) Certifications under § 164.518(b); and

(9) Complaints received and any responses thereto pursuant to § 164.518(d).

(g) *Implementation specification: Change in policy or procedure.* (1) Except as provided in paragraph (g)(2) of this section, a covered entity may not implement a change to a policy or procedure required or permitted under this subpart until it has made the appropriate changes to the documentation required by this section and the notice required by § 164.512.

(2) Where the covered entity determines that a compelling reason exists to make a use or disclosure or take another action permitted under this subpart that its notice and policies and procedures do not permit, it may make the use or disclosure or take the other action if:

(1) It documents the reasons supporting the use, disclosure, or other action; and

(2) Within 30 days of the use, disclosure, or other action, changes its notice, policies and procedures to permit such use, disclosure, or other action.

§ 164.522 Compliance and enforcement.

(a) *Principles for achieving compliance.*—(1) *Cooperation.* The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the requirements established under this subpart.

(2) *Assistance.* The Secretary may provide technical assistance to covered entities to help them comply voluntarily with this subpart.

(b) *Individual complaints to the Secretary.* An individual who believes that a covered entity is not complying with the requirements of this subpart may file a complaint with the Secretary, provided that, where the complaint relates to the alleged failure of a covered entity to amend or correct protected health information pursuant to § 164.516, the Secretary may determine whether the covered entity has followed procedures that comply with § 164.516, but will not determine whether the information involved is accurate, complete, or whether errors or omissions might have an adverse effect on the individual.

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

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

(ii) A complaint should name the entity that is the subject of the complaint and describe in detail the acts or omissions believed to be in violation of the requirements of this subpart.

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

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

(c) *Compliance reviews.* The Secretary may conduct compliance reviews to determine whether covered entities are complying with this subpart.

(d) *Responsibilities of covered entities.*—(1) *Provide records and compliance reports.* A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the requirements of this subpart.

(2) *Cooperate with periodic compliance reviews.* The covered entity shall cooperate with the Secretary if the Secretary undertakes a review of the policies, procedures, and practices of a covered entity to determine whether it is complying with this subpart.

(3) *Permit access to information.* A covered entity must permit access by the Secretary during normal business hours to its books, records, accounts, and other sources of information, including protected health information, and its facilities, that are pertinent to ascertaining compliance with this subpart. Where any information required of a covered entity under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity must so certify and set forth what efforts it has made to obtain the information. Protected health information obtained in connection with a compliance review or investigation under this subpart will not be disclosed by the Secretary, except where necessary to enable the Secretary to ascertain compliance with this subpart, in formal enforcement proceedings, or where otherwise required by law.

(4) *Refrain from intimidating or retaliatory acts.* A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the filing of a complaint under this section, for testifying, assisting, participating in any manner in an investigation, compliance review, proceeding or hearing under this Act, or opposing any act or practice made unlawful by this subpart.

(e) *Secretarial action regarding complaints and compliance reviews.*—(1) *Resolution where noncompliance is indicated.* (i) If an investigation pursuant to paragraph (b)(2) of this section or a compliance review pursuant to paragraph (c) of this section indicates a failure to comply, the Secretary will so inform the covered entity and, where the matter arose from a complaint, the individual, and resolve the matter by informal means whenever possible.

(ii) If the Secretary determines that the matter cannot be resolved by informal means, the Secretary may issue written findings documenting the non-compliance to the covered entity and, where the matter arose from a complaint, to the complainant. The Secretary may use such findings as a basis for initiating action under section 1176 of the Act or initiating a criminal referral under section 1177.

(2) *Resolution where no violation is found.* If an investigation or compliance review does not warrant action pursuant

to paragraph (e)(1) of this section, the Secretary will so inform the covered entity and, where the matter arose from a complaint, the individual in writing.

§ 164.524 Effective date.

A covered entity must be in compliance with this subpart not later than 24 months following the effective date of this rule, except that a covered entity that is a small health plan must be in compliance with this subpart not later than 36 months following the effective date of the rule.

Appendix to Subpart E of Part 164—Model Authorization Form

AUTHORIZATION FOR RELEASE OF INFORMATION

Section A: Must be completed for all authorizations

I hereby authorize the use or disclosure of my individually identifiable health information as described below. I understand that this authorization is voluntary. I understand that if the organization authorized to receive the informatior is not a health plan or health care provider, the released information may no longer be protected by federal privacy regulations.

Patient name: _____ **ID Number:** _____

Persons/organizations providing the information:	**Persons/organizations receiving the information:**
_____	_____
_____	_____
_____	_____
_____	_____

Specific description of information (including date(s)): _____

_____

_____

_____

_____

Section B: Must be completed only if a health plan or a health care provider has requested the authorization

1. The health plan or health care provider must complete the following:
   a. What is the purpose of the use or disclosure?: _____
   _____
   b. Will the health plan or health care provider requesting the authorization receive financial or in-kind compensation in exchange for using or disclosing the health information described above? Yes_____ No_____

2. The patient or the patient's representative must read and initial the following statements:
   a. I understand that my health care and the payment for my health care will not be affected if I do not sign this form. Initials: _____
   b. I understand that I may see and copy the information described on this form if I ask for it, and that I get a copy of this form after I sign it. Initials: _____

Section C: Must be completed for all authorizations

The patient or the patient's representative must read and initial the following statements:

1. I understand that this authorization will expire on __ __/__ __/__ __ __ __ (DD/MM/YR) Initials: _____
2. I understand that I may revoke this authorization at any time by notifying the providing organization in writing, but if I do it won't have any affect on any actions they took before they received the revocation. Initials: _____

_____ _____

Signature of patient or patient's representative **Date**

(Form MUST be completed before signing.)

Printed name of patient's representative: _____

Relationship to the patient: _____

**** YOU MAY REFUSE TO SIGN THIS AUTHORIZATION ****

You may not use this form to release information for treatment or payment except when the information to be released is psychotherapy notes or certain research information.

[FR Doc. 99–28440 Filed 10–28–99; 4:45 pm]

BILLING CODE 4150–04–C