from national surveys while preserving confidentiality and which have been dealing with these issues for decades. The problems and solutions being used by these agencies are laid out in detail in the Statistical Policy Working Paper 22 cited earlier.

To protect the privacy of individuals providing information to the Bureau of Census, the Bureau has determined that a geographical region must contain at least 100,000 people.[20] This standard has been used by the Bureau of the Census for many years and is supported by simulation studies using Census data.[21] These studies showed that after a certain point, increasing the size of a geographic area does not significantly decrease the percentage of unique records (i.e., those that could be identified if sampled), but that the point of diminishing returns is dependent on the number and type of demographic variables on which matching might occur. For a small number of demographic variables (6), this point was quite low (about 20,000 population), but it rose quickly to about 50,000 for 10 variables and to about 80,000 for 15 variables. The Bureau of the Census releases sets of data to the public that it considers safe from re-identification because it limits geographical areas to those containing at least 100,000 people and limits the number and detail of the demographic variables in the data. At the point of approximately 100,000 population, 7.3% of records were unique (and therefore potentially identifiable) on 6 demographic variables from the 1990 Census Short Form: Age in years (90 categories), race (up to 180 categories), sex (2 categories), relationship to householder (14 categories), Hispanic (2 categories), and tenure (owner vs. renter in 5 categories). Using 6 variables derived from the Long Form data, age (10 categories), race (6 categories), sex (2 categories), marital status (5 categories), occupation (54 categories), and personal income (10 categories), raised the percentage to 9.8%.

We also examined the results of an NCHS simulation study using national survey data[22] to see if some scientific support could be found for a compromise. The study took random samples from populations of different sizes and then compared the samples to the whole population to see how many records were identifiable, that is, matched uniquely to a unique person in the whole population on the basis of 9 demographic variables: Age (85 categories), race (4 categories), gender (2 categories), ethnicity (2 categories), marital status (3 categories), income (3 categories), employment status (2 categories), working class (4 categories), and occupation (42 categories). Even when some of the variables are aggregated or coded, from the perspective of a large statistical agency desiring to release data to the public, the study concluded that a population size of 500,000 was not sufficient to provide a reasonable guarantee that certain individuals could not be identified. About 2.5 % of the sample from the population of 500,000 was uniquely identifiable, regardless of sample size. This percentage rose as the size of the population decreased, to about 14% for a population of 100,000 and to about 25% for a population of 25,000. Eliminating the occupation variable (which is less likely to be found in health data) reduced this percentage significantly to about 0.4 %, 3%, and 10% respectively. These percentages of unique records (and thus the potentials for re-identification) are highly dependent on the number of variables (which must also be available in other databases which are identified to be considered in a disclosure risk analysis), the categorical breakdowns of those variables, and the level of geographic detail included.

With respect to how we might clarify the requirement to achieve a ''low probability'' that information could be identified, the Statistical Policy Working Paper 22 referenced above discusses the attempts of several researchers to define mathematical measures of disclosure risk only to conclude that ''more research into defining a computable measure of risk is necessary.'' When we considered whether we could specify a maximum level of risk of disclosure with some precision (such as a probability or risk of identification of <0.01), we concluded that it is premature to assign mathematical precision to the ''art'' of de-identification.

After evaluating current practices and recognizing the expressed need for some geographic indicators in otherwise de-identified databases, we concluded that permitting geographic identifiers that define populations of greater than 20,000 individuals is an appropriate standard that balances privacy interests against desirable uses of de-identified data. In making this determination, we focused on the studies by the Bureau of Census cited above which seemed to indicate that a population size of 20,000 was an appropriate cut off if there were relatively few (6) demographic variables in the database. Our belief is that, after removing the required identifiers to meet the safe harbor standards, the number of demographic variables retained in the databases will be relatively small, so that it is appropriate to accept a relatively low number as a minimum geographic size.

In applying this provision, covered entities must replace the (currently 18) forbidden 3-digit zip codes with zeros and thus treat them as a single geographic area (with >20,000 population). The list of the forbidden 3-digit zip codes will be maintained as part of the updated Secretarial guidance referred to above. Currently, they are: 022, 036, 059, 102, 203, 555, 556, 692, 821, 823, 830, 831, 878, 879, 884, 893, 987, and 994. This will result in an average 3-digit zip code area population of 287,858 which should result in an average of about 4% unique records using the 6 variables described above from the Census Short Form. Although this level of unique records will be much higher in the smaller geographic areas, the actual risk of identification will be much lower because of the limited availability of comparable data in publically available, identified databases, and will be further reduced by the low probability that someone will expend the resources to try to identify records when the chance of success is so small and uncertain. We think this compromise will meet the current need for an easy method to identify geographic area while providing adequate protection from re-identification. If a greater level of geographical detail is required for a particular use, the information will have to be obtained through another permitted mechanism or be subjected to a specific de-identification determination as described above. We will monitor the availability of identified public data and the concomitant re-identification risks, both theoretical and actual, and adjust this safe harbor in the future as necessary.

As we stated above, we understand that many commenters would prefer a looser standard for determining when information is de-identified, both generally and with respect to the standards for identifying geographic

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

[21] The Geographic Component of Disclosure Risk for Microdata. Brian Greenberg and Laura Voshell. Bureau of the Census Statistical Research Division Report: Census/SRD/RR–90–13, October, 1990.

[22] A Simulation Study of the Identifiability of Survey Respondents when their Community of Residence is Known. John Horm, Natonal Center for Health Statistics, 2000.

area. However, because public databases (such as voter records or driver's license records) that include demographic information about a geographically defined population are available, a surprisingly large percentage of records of health information that contain similar demographic information can be identified. Although the number of these databases seems to be increasing, the number of demographic variables within them still appears to be fairly limited. The number of cases of privacy violation from health records which have been identified in this way is small to date. However, the risk of identification increases with decreasing population size, with increasing amounts of demographic information (both in level of detail and number of variables), and with the uniqueness of the combination of such information in the population. That is, an 18-year-old single white male student is not at risk of identification in a database from a large city such as New York. However, if the database were about a small town where most of the inhabitants were older, retired people of a specific minority race or ethnic group, that same person might be unique in that community and easily identified. We believe that the policy that we have articulated reaches the appropriate balance between reasonably protecting privacy and providing a sufficient level of information to make de-identified databases useful.

Comments: Some comments noted that identifiers that accompany photographic images are often needed to interpret the image and that it would be difficult to use the image alone to identify the individual.

Response: We agree that our proposed requirement to remove all photographic images was more than necessary. Many photographs of lesions, for example, which cannot usually be used alone to identify an individual, are included in health records. In this final rule, the only absolute requirement is the removal of full-face photographs, and we depend on the ''catch-all'' of ''any other unique * * * characteristic * * * '' to pick up the unusual case where another type of photographic image might be used to identify an individual.

Comments: A number of commenters felt that the proposed bar for removal had been set too high; that the removal of these 19 identifiers created a difficult standard, since some identifiers may be buried in lengthy text fields.

Response: We understand that some of the identifiers on our list for removal may be buried in text fields, but we see no alternative that protects privacy. In addition, we believe that such unstructured text fields have little or no value in a de-identified information set and would be removed in any case. With time, we expect that such identifiers will be kept out of places where they are hard to locate and expunge.

Comments: Some commenters asserted that this requirement creates a disincentive for covered entities to de-identify data and would compromise the Secretary's desire to see de-identified data used for a multitude of purposes. Others stated that the ''no reason to believe'' test creates an unreasonable burden on covered entities, and would actually chill the release of de-identified information, and set an impossible standard.

Response: We recognize that the proposed standards might have imposed a burden that could have prevented the widespread use of de-identified information. We believe that our modifications to the final rule discussed above will make the process less burdensome and remove some of the disincentive. However, we could not loosen the standards as far as many commenters wanted without seriously jeopardizing the privacy of the subjects of the information. As discussed above, we modify the ''no reason to know'' standard that was part of the safe harbor provision and replace it in the final rule with an ''actual knowledge'' standard. We believe that this change provides additional certainty to covered entities using the safe harbor and should eliminate any chilling effect.

Comments: Although most commenters wanted to see data elements taken off the list, there were a small number of commenters that wanted to see data items added to the list. They believed that it is also necessary to remove clinical trial record numbers, device model serial numbers, and all proper nouns from the records.

Response: In response to these requests, we have slightly revised the list of identifiers that must be removed under the safe harbor provision. Clinical trial record numbers are included in the general category of ''any other unique identifying number, characteristic, or code.'' These record numbers cannot be included with de-identified information because, although the availability of clinical trial numbers may be limited, they are used for other purposes besides de-identification/re-identification, such as identifying clinical trial records, and may be disclosed under certain circumstances. Thus, they do not meet the criteria in the rule for use as a unique record identifier for de-identified records. Device model serial numbers are included in ''any device identifier or serial number'' and must be removed. We considered the request to remove all proper nouns to be very burdensome to implement for very little increase in privacy and likely to be arbitrary in operation, and so it is not included in the final rule.

Re-Identification

Comments: One commenter wanted to know if the rule requires that covered entities retain the ability to re-identify de-identified information.

Response: The rule does not require covered entities to retain the ability to re-identify de-identified information, but it does allow them to retain this ability.

Comments: A few commenters asked us to prohibit anyone from re-identifying de-identified health information.

Response: We do not have the authority to regulate persons other than covered entities, so we cannot affect attempts by entities outside of this rule to re-identify information. Under the rule, we permit the covered entity that created the de-identified information to re-identify it. However, we include a requirement that, when a unique record identifier is included in the de-identified information, such identifier must not be such that someone other than the covered entity could use it to identify the individual (such as when a derivative of the individual's name is used as the unique record identifier).

Section 164.514(d)—Minimum Necessary

Comment: A large number of commenters objected to the application of the proposed ''minimum necessary'' standard for uses and disclosures of protected health information to uses and disclosures for treatment purposes. Some suggested that the final regulation should establish a good faith exception or safe harbor for disclosures made for treatment.

The overwhelming majority of commenters, generally from the medical community, argued that application of the proposed standard would be contrary to sound medical practice, increase medical errors, and lead to an increase in liability. Some likened the standard to a ''gag clause'' in that it limited the exchange of information critical for quality patient care. They found the standard unworkable in daily treatment situations. They argued that this standard would be potentially dangerous in that it could cause practitioners to withhold information that could be essential for later care. Commenters asserted that caregivers need to be able to give and receive a

complete picture of the patient's health to make a diagnosis and develop a treatment plan.

Other commenters noted that the complexity of medicine is such that it is unreasonable to think that anyone will know the exact parameters of the information another caregiver will need for proper diagnosis and treatment or that a plan will need to support quality assurance and improvement activities. They therefore suggested that the minimum necessary standard be applied instead as an administrative requirement.

Providers also emphasized that they already have an ethical duty to limit the sharing of unnecessary medical information, and most already have well-developed guidelines and practice standards in place. Concerns were also voiced that attempts to provide the minimum necessary information in the treatment setting would lead to multiple editions of a record or creation of summaries that turn out to omit crucial information resulting in confusion and error.

Response: In response to these concerns, we substantially revise the minimum necessary requirements. As suggested by certain commenters, we provide, in § 164.502(b), that disclosures of protected health information to or requests by health care providers for treatment are not subject to the minimum necessary standard. We also modify the requirements for uses of protected health information. This final rule requires covered entities to make determinations of minimum necessary use, including use for treatment purposes, based on the role of the person or class of workforce members rather than at the level of specific uses. A covered entity must establish policies and procedures that identify the types of persons who are to have access to designated categories of information and the conditions, if any, of that access. We establish no requirements specific to a particular use of information. Covered entities are responsible for establishing and documenting these policies and procedures. This approach is consistent with the argument of many commenters that guidelines and practice standards are appropriate means for protecting the privacy of patient information.

Comment: Some commenters argued that the standard should be retained in the treatment setting for uses and disclosures pertaining to mental health information. Some of these commenters asserted that other providers do not need to know the mental status of a patient for treatment purposes.

Response: We agree that the standard should be retained for uses of mental health information in the treatment setting. However, we believe that the arguments for excepting disclosures of protected health information for treatment purposes from application of the minimum necessary standard are also persuasive with respect to mental health information. An individual's mental health can interact with proper treatment for other conditions in many ways. Psychoactive medications may have harmful interactions with drugs routinely prescribed for other purposes; an individual's mental health history may help another health care provider understand the individual's ability to abide by a complicated treatment regimen. For these reasons, it is also not reasonable to presume that, in every case, a health care provider will not need to know an individual's mental health status to provide appropriate treatment.

Providers' comments noted existing ethical duties to limit the sharing of unnecessary medical information, and well-developed guidelines and practice standards for this purpose. Under this rule, providers may use these tools to guide their discretion in disclosing health information for treatment.

Comment: Several commenters urged that covered entities should be required to conspicuously label records to show that they are not complete. They argued that absent such labeling, patient care could be compromised.

Response: We believe that the final policy to except disclosures of protected health information for treatment purposes from application of the minimum necessary standard addresses these commenters' concerns.

Comment: Some commenters argued that the audit exception to the minimum necessary requirements needs to be clarified or expanded, because ''audit'' and ''payment'' are essentially the same thing.

Response: We eliminate this exception. The proposed exclusion of disclosures to health plans for audit purposes is replaced with a general requirement that covered entities must limit requests to other covered entities for individually identifiable health information to what is reasonably necessary for the purpose intended.

Comment: Many commenters argued that the proposed standard was unworkable as applied to ''uses'' by a covered entity's employees, because the proposal appeared not to allow providers to create general policy as to the types of records that particular employees may have access to but instead required that each decision be made ''individually,'' which providers interpret as ''case-by-case.'' Commenters argued that the standard with regard to ''uses'' would be impossible to implement and prohibitively expensive, requiring both medical and legal input to each disclosure decision.

Some commenters recommended deletion of the minimum necessary standard with regard to ''uses.'' Other commenters specifically recommended deletion of the requirement that the standard be applied on an individual, case-by-case basis. Rather, they suggested that the covered entity be allowed to establish general policies to meet the requirement. Another commenter similarly urged that the standard not apply to internal disclosures or for internal health care operations such as quality improvement/assurance activities. The commenter recommended that medical groups be allowed to develop their own standards to ensure that these activities are carried out in a manner that best helps the group and its patients.

Other commenters expressed confusion and requested clarification as to how the standard as proposed would actually work in day-to-day operations within an entity.

Response: Commenters' arguments regarding the workability of this standard as proposed were persuasive, and we therefore make significant modification to address these comments and improve the workability of the standard. For all uses and many disclosures, we require covered entities to include in their policies and procedures (see § 164.530), which may be standard protocols, for ''minimum necessary'' uses and disclosures. We require implementation of such policies in lieu of making the ''minimum necessary'' determination for each separate use and disclosure.

For uses, covered entities must implement policies and procedures that restrict access to and use of protected health information based on the specific professional roles of members of the covered entity's workforce. The policies and procedures must identify the persons or classes of persons in the entity's workforce who need access to protected health information to carry out their duties and the category or categories of protected health information to which such persons or classes need access. These role-based access rules must also identify the conditions, as appropriate, that would apply to such access. For example, an institutional health care provider could allow physicians access to all records under the condition that the viewing of medical records of patients not under their care is recorded and reviewed. Other health professionals' access could

be limited to time periods when they are on duty. Information available to staff who are responsible for scheduling surgical procedures could be limited to certain data. In many instances, use of order forms or selective copying of relevant portions of a record may be appropriate policies to meet this requirement.

Routine disclosures also are not subject to individual review; instead, covered entities must implement policies and procedures (which may be standard protocols) to limit the protected health information in routine disclosures to the minimum information reasonably necessary to achieve the purpose of that type of disclosure. For non-routine disclosures, a covered entity must develop reasonable criteria to limit the protected health information disclosed to the minimum necessary to accomplish the purpose for which disclosure is sought, and to implement procedures for review of disclosures on an individual basis.

We modify the proposed standard to require the covered entity to make ''reasonable efforts'' to meet the minimum necessary standard (not ''all'reasonable efforts, as proposed). What is reasonable will vary with the circumstances. When it is practical to use order forms or selective copying of relevant portions of the record, the covered entity is required to do so. Similarly, this flexibility in the standard takes into account the ability of the covered entity to configure its record system to allow selective access to only certain fields, and the practicality of organizing systems to allow this capacity. It might be reasonable for a covered entity with a highly computerized information system to implement a system under which employees with certain functions have access to only limited fields in a patient records, while other employees have access to the complete records. Such a system might not be reasonable for a covered entity with a largely paper records system.

Covered entities' policies and procedures must provide that disclosure of an entire medical record will not be made except pursuant to policies which specifically justify why the entire medical record is needed.

We believe that these modifications significantly improve the workability of this standard. At the same time, we believe that asking covered entities to assess their practices and establish rules for themselves will lead to significant improvements in the privacy of health information. See the preamble for § 164.514 for a more detailed discussion.

Comment: The minimum necessary standard should not be applied to uses and disclosures for payment or health care operations.

Response: Commenter's arguments for exempting these uses and disclosures from the minimum necessary standard were not compelling. We believe that our modifications to application of the minimum necessary standard to internal uses of protected health information, and to routine disclosures, address many of the concerns raised, particularly the concerns about administrative burdens and the concerns about having the information necessary for day-to-day operations. We do not eliminate this standard in part because we also remain concerned that covered entities may be tempted to disclose an entire medical record when only a few items of information are necessary, to avoid the administrative step of extracting the necessary information (or redacting the unnecessary information). We also believe this standard will cause covered entities to assess their privacy practices, give the privacy interests of their patients and enrollees greater attention, and make improvements that might otherwise not have been made. For this reason, the privacy benefits of retaining the minimum necessary standard for these purposes outweigh the burdens involved. We note that the minimum necessary standard is tied to the purpose of the disclosure; thus, providers may disclose protected health information as necessary to obtain payment.

Comment: Other commenters urged us to apply a ''good faith'' provision to all disclosures subject to the minimum necessary standard. Commenters presented a range of options to modify the proposed provisions which, in their view, would have mitigated their liability if they failed to comply with minimum necessary standard.

Response: We believe that the modifications to this standard, described above, substantially address these commenters' concerns. In addition to allowing the covered entity to use standard protocols for routine disclosures, we modify the standard to require a covered entity to make ''reasonable efforts,'' not ''all'' reasonable efforts as proposed, in making the ''minimum necessary'' disclosure.

Comments: Some commenters complained that language in the proposed rule was vague and provided little guidance, and should be abandoned.

Response: In the preamble for § 164.504 and these responses to comments, we provide further guidance on how a covered entity can develop its policies for the minimum necessary use and disclosure of protected health information. We do not abandon this standard for the reasons described above. We remain concerned about the number of persons who have access to identifiable health information, and believe that causing covered entities to examine their practices will have significant privacy benefits.

Comment: Some commenters asked that the minimum necessary standard should not be applied to disclosures to business partners. Many of these commenters articulated the burdens they would bear if every disclosure to a business partner was required to meet the minimum necessary standard.

Response: We do not agree. In this final rule, we minimize the burden on covered entities in the following ways: in circumstances where disclosures are made on a routine, recurring basis, such as in on-going relationships between covered entities and their business associates, individual review of each routine disclosure has been eliminated; covered entities are required only to develop standard protocols to apply to such routine disclosures made to business associates (or types of business associates). In addition, we allow covered entities to rely on the representation of a professional hired to provide professional services as to what information is the minimum necessary for that purpose.

Comment: Some commenters were concerned that applying the standard in research settings will result in providers declining to participate in research protocols.

Response: We have modified the proposal to reduce the burden on covered entities that wish to disclose protected health information for research purposes. The final rule requires covered entities to obtain documentation or statements from persons requesting protected health information for research that, among other things, describe the information necessary for the research. We allow covered entities to reasonably rely on the documentation or statements as describing the minimum necessary disclosure.

Comment: Some commenters argued that government requests should not be subject to the minimum necessary standard, whether or not they are ''authorized by law.''

Response: We found no compelling reason to exempt government requests from this standard, other than when a disclosure is required by law. (See preamble to § 164.512(a) for the

rationale behind this policy). When a disclosure is required by law, the minimum necessary standard does not apply, whether the recipient of the information is a government official or a private individual.

At the same time, we understand that when certain government officials make requests for protected health information, some covered entities might feel pressure to comply that might not be present when the request is from a private individuals. For this reason, we allow (but do not require) covered entities to reasonably rely on the representations of public officials as to the minimum necessary information for the purpose.

Comment: Some commenters argued that requests under proposed § 164.510 should not be subject to the minimum necessary standard, whether or not they are ''authorized by law.'' Others argued that for disclosures made for administrative proceedings pursuant to proposed § 164.510, the minimum necessary standard should apply unless they are subject to a court order.

Response: We found no compelling reason to exempt disclosures for purposes listed in the regulation from this standard, other than for disclosures required by law. When there is no such legal mandate, the disclosure is voluntary on the part of the covered entity, and it is therefore reasonable to expect the covered entity to make some effort to protect privacy before making such a disclosure. If the covered entity finds that redacting unnecessary information, or extracting the requested information, prior to making the disclosure, is too burdensome, it need not make the disclosure. Where there is ambiguity regarding what information is needed, some effort on the part of the covered entity can be expected in these circumstances.

We also found no compelling reason to limit the exemption for disclosures ''required by law'' to those made pursuant to a court order. The judgment of a state legislature or regulatory body that a disclosure is required is entitled to no less deference than the same decision made by a court. For further rationale for this policy, see the preamble to § 164.512(a).

Comment: Some commenters argued that, in cases where a request for disclosure is not required by law, covered entities should be permitted to rely on the representations by public officials, that they have requested no more than the minimum amount necessary.

Response: We agree, and retain the proposed provision which allows reasonable reliance on the representations of public officials.

Comment: Some commenters argued that it is inappropriate to require covered entities to distinguish between disclosures that are ''required by law'' and those that are merely ''authorized by law,'' for the purposes of determining when the standard applies.

Response: We do not agree. Covered entities have an independent duty to be aware of their legal obligations to federal, state, local and territorial or tribal authorities. In addition, § 164.514(h) allows covered entities to reasonably rely on the oral or written representation of public officials that a disclosure is required by law.

Comment: The minimum necessary standard should not be applied to pharmacists, or to emergency services.

Response: We believe that the final rule's exemption of disclosures of protected health information to health care providers for treatment purposes from the minimum necessary standard addresses these commenters concerns about emergency services. Together with the other changes we make to the proposed standard, we believe we have also addressed most of the commenters' concerns about pharmacists. With respect to pharmacists, the comments offered no persuasive reasons to treat pharmacists differently from other health care providers. Our reasons for retaining this standard for other uses and disclosures of protected health information are explained above.

Comment: A number of commenters argued that the standard should not apply to disclosures to attorneys, because it would interfere with the professional duties and judgment of attorneys in their representation of covered entities. Commenters stated that if a layperson within a covered entity makes an improper decision as to what the minimum necessary information is in regard to a request by the entity's attorney, the attorney may end up lacking information that is vital to representation. These commenters stated that attorneys are usually going to be in a better position to determine what information is truly the minimum necessary for effective counsel and representation of the client.

Response: We found no compelling reason to treat attorneys differently from other business associates. However, to ensure that this rule does not inadvertently cause covered entities to second-guess the professional judgment of the attorneys and other professionals they hire, we modify the proposed policies to explicitly allow covered entities to rely on the representation of a professional hired to provide professional services as to what information is the minimum necessary for that purpose.

Comment: Commenters from the law enforcement community expressed concern that providers may attempt to misuse the minimum necessary standard as a means to restrict access to information, particularly with regard to disclosures for health oversight or to law enforcement officials.

Response: The minimum necessary standard does not apply to disclosures required by law. Since the disclosures to law enforcement officials to which this standard applies are all voluntary, there would be no need for a covered entity to ''manipulate'' the standard; it could decline to make the disclosure.

Comment: Some commenters argued that the only exception to the application of the standard should be when an individual requests access to his or her own information. Many of these commenters expressed specific concerns about victims of domestic violence and other forms of abuse.

Response: We do not agree with the general assertion that disclosure to the individual is the only appropriate exception to the minimum necessary standard. There are other, limited, circumstances in which application of the minimum necessary standard could cause significant harm. For reasons described above, disclosures of protected health information for treatment purposes are not subject to this standard. Similarly, as described in detail in the preamble to § 164.512(a), where another public body has mandated the disclosure of health information, upsetting that judgment in this regulation would not be appropriate.

The more specific concerns expressed about victims of domestic violence and other forms of abuse are addressed in a new provision regarding disclosure of protected health information related to domestic violence and abuse (see § 164.512(c)), and in new limitations on disclosures to persons involved in the individual's care (see § 164.510(b)). We believe that the limitations we place on disclosure of health information in those circumstances address the concerns of these commenters.

Comment: Some commenters argued that disclosures to next of kin should be restricted to minimum necessary protected health information, and to protected health information about only the current medical condition.

Response: In the final regulation, we change the proposed provision regarding ''next of kin'' to more clearly focus on the disclosures we intended to target: Disclosures to persons involved

in the individual's care. We allow such disclosure only with the agreement of the individual, or where the covered entity has offered the individual the opportunity to object to the disclosure and the individual did not object. If the opportunity to object cannot practicably be provided because of the incapacity of the individual or other emergency, we require covered entities to exercise professional judgment in the best interest of the patient in deciding whether to disclose information. In such cases, we permit disclosure only of that information directly relevant to the person's involvement with the individual's health care. (This provision also includes limited disclosure to certain persons seeking to identify or locate an individual.) See § 164.510(b).

Some additional concerns expressed about victims of domestic violence and other forms of abuse are also addressed in a new section on disclosure of protected health information related to domestic violence and abuse. See § 164.512(c). We believe that the limitations we place on disclosure of health information in these provisions address the concerns of these commenters.

Comment: Some commenters argued that covered entities should be required to determine whether de-identified information could be used before disclosing information under the minimum necessary standard.

Response: We believe that requiring covered entities' policies and procedures for minimum necessary disclosures to address whether de-identified information could be used in all instances would impose burdens on some covered entities that could outweigh the benefits of such a requirement. There is significant variation in the sophistication of covered entities' information systems. Some covered entities can reasonably implement policies and procedures that make significant use of de-identified information; other covered entities would find such a requirement excessively burdensome. For this reason, we chose instead to require ''reasonable efforts,'' which can vary according to the situation of each covered entity.

In addition, we believe that the fact that we allow de-identified information to be disclosed without regard to the policies, procedures, and documentation required for disclosure of identifiable health information will provide an incentive to encourage its use where appropriate.

Comment: Several commenters argued that standard transactions should not be subject to the standard.

Response: We agree that data elements that are required or situationally required in the standard transactions should not be, and are not, subject to this standard. However, in many cases, covered entities have significant discretion as to the information included in these transactions. Therefore, this standard does apply to those optional data elements.

Comment: Some commenters asked for clarification to understand how the minimum necessary standard is intended to interact with the security NPRM.

Response: The proposed Security Rule included requirements for electronic health information systems to include access management controls. Under this regulation, the covered entity's privacy policies will determine who has access to what protected health information. We will make every effort to ensure consistency prior to publishing the final Security Rule.

Comment: Many commenters, representing health care providers, argued that if the request was being made by a health plan, the health plan should be required to request only the minimum protected health information necessary. Some of these commenters stated that the requestor is in a better position to know the minimum amount of information needed for their purposes. Some of these commenters argued that the minimum necessary standard should be imposed only on the requesting entity. A few of these commenters argued that both the disclosing and the requesting entity should be subject to the minimum necessary standard, to create ''internal tension'' to assure the standard is honored.

Response: We agree, and in the final rule we require that a request for protected health information made by one covered entity to another covered entity must be limited to the minimum amount necessary for the purpose. As with uses and disclosures of protected health information, covered entities may have standard protocols for routine requests. Similarly, this requirement does not apply to requests made to health care providers for treatment purposes. We modify the rule to balance this provision; that is, it now applies both to disclosure of and requests for protected health information. We also allow, but do not require, the covered entity releasing the information to reasonably rely on the assertion of a requesting covered entity that it is requesting only the minimum protected health information necessary.

Comment: A few commenters suggested that there should be a process for resolving disputes between covered entities over what constitutes the ''minimum necessary'' information.

Response: We do not intend that this rule change the way covered entities currently handle their differences regarding the disclosure of health information. We understand that the scope of information requested from providers by health plans is a source of tension in the industry today, and we believe it would not be appropriate to use this regulation to affect that debate. As discussed above, we require both the requesting and the disclosing covered entity to take privacy concerns into account, but do not inject additional tension into the on-going discussions.

Section 164.514(e)—Marketing

Comment: Many commenters requested clarification of the boundaries between treatment, payment, health care operations, and marketing. Some of these commenters requested clarification of the apparent inconsistency between language in proposed § 164.506(a)(1)(i) (a covered entity is permitted to use or disclose protected health information without authorization ''to carry out'' treatment, payment, or health care operations) and proposed § 164.508(a)(2)(A) (a covered entity must obtain an authorization for all uses and disclosures that are not ''compatible with or directly related to'' treatment, payment, and health care operations). They suggested retaining the language in proposed § 164.508(a)(2)(A), which would permit a broader range of uses and disclosures without authorization, in order to engage in health promotion activities that might otherwise be considered marketing.

Response: In the final rule, we make several changes to the definitions of treatment, payment, and health care operations that are intended to clarify the uses and disclosures of protected health information that may be made for each purpose. See § 164.501 and the corresponding preamble discussion regarding the definitions of these terms. We also have added a definition of the term ''marketing'' to help establish the boundary between marketing and treatment, payment, and health care operations. See § 164.501. We also clarify the conditions under which authorization is or is not required for uses and disclosures of protected health information for marketing purposes. See § 164.514(e). Due to these changes, we believe it is appropriate to retain the wording from proposed § 164.506(a)(1)(i).

Comment: We received a wide variety of suggestions with respect to authorization for uses and disclosures of protected health information for marketing purposes. Some commenters supported requiring authorization for all such uses and disclosures. Other commenters suggested permitting all such uses and disclosures without authorization.

Some commenters suggested we distinguish between marketing to benefit the covered entity and marketing to benefit a third party. For example, a few commenters suggested we should prohibit covered entities from seeking authorization for any use or disclosure for marketing purposes that benefit a third party. These commenters argued that the third parties should be required to obtain the individual's authorization directly from the individual, not through a covered entity, due to the potential for conflicts of interest.

While a few commenters suggested that we require covered entities to obtain authorization to use or disclose protected health information for the purpose of marketing its own products and services, the majority argued these types of marketing activities are vital to covered entities and their customers and should therefore be permitted to occur without authorization. For example, commenters suggested covered entities should be able to use and disclose protected health information without authorization in order to provide appointment reminders, newsletters, information about new initiatives, and program bulletins.

Finally, many commenters argued we should not require authorization for the use or disclosure of protected health information to market any health-related goods and services, even if those goods and services are offered by a third party. Some of these commenters suggested that individuals should have an opportunity to opt out of these types of marketing activities rather than requiring authorization.

Response: We have modified the final rule in ways that address a number of the issues raised in the comments. First, the final rule defines the term marketing, and excepts certain communications from the definition. See § 164.501. These exceptions include communications made by covered entities for the purpose of describing network providers or other available products, services, or benefits and communications made by covered entities for certain treatment-related purposes. These exceptions only apply to oral communications or to written communications for which the covered entity receives no third-party remuneration. The exceptions to the definition of marketing fall within the definitions of treatment and/or health care operations, and therefore uses, or disclosures to a business associate, of protected health information for these purposes are permissible under the rule without authorization.

The final rule also permits covered entities to use protected health information to market health-related products and services, whether they are the products and services of the covered entity or of a third party, subject to a number of limitations. See § 164.514(e). We permit these uses to allow entities in the health sector to inform their patients and enrollees about products that may benefit them. The final rule contains significant restrictions, including requirements that the covered entity disclose itself as the source of a marketing communication, that it disclose any direct or indirect remuneration from third parties for making the disclosure, and that, except in the cases of general communications such as a newsletter, the communication disclose how the individual can opt-out of receiving additional marketing communications. Additional requirements are imposed if the communication is targeted based on the health status or condition of the proposed recipients.

We believe that these modifications address many of the issues raised by commenters and provide a substantial amount of flexibility as to when a covered entity may communicate about a health-related product or service to a patient or enrollee. These communications may include appointment reminders, newsletters, and information about new health products. These changes, however, do not permit a covered entity to disclose protected health information to third parties for marketing (other than to a business associate to make a marketing communication on behalf of the covered entity) without authorization under § 164.508.

Comment: A few commenters suggested we prohibit health care clearinghouses from seeking authorization for the use or disclosure of protected health information for marketing purposes.

Response: We do not prohibit clearinghouses from seeking authorizations for these purposes. We believe, however, that health care clearinghouses will almost always create or obtain protected health information in a business associate capacity. Business associates may only engage in activities involving the use or disclosure of protected health information, including seeking or acting on an authorization, to the extent their contracts allow them to do so. When a clearinghouse creates or receives protected health information other than as a business associate of a covered entity, it is permitted and required to obtain authorizations to the same extent as any other covered entity.

Comment: A few commenters suggested we require covered entities to publicly disclose, on the covered entity's website or upon request, all of their marketing arrangements.

Response: While we agree that such a requirement would provide individuals with additional information about how their information would be used, we do not feel that such a significant intrusion into the business practices of the covered entity is warranted.

Comment: Some commenters argued that if an activity falls within the scope of payment, it should not be considered marketing. Commenters strongly supported an approach which would bar an activity from being construed as ''marketing'' even if performing that activity would result in financial gain to the covered entity. In a similar vein, we were urged to adopt the position that if an activity was considered payment, treatment or health care operations, it could not be further evaluated to determine whether it should be excluded as marketing.

Response: We considered the approach offered by commenters but decided against it. Some activities, such as the marketing of a covered entity's own health-related products or services, are now included in the definition of health care operations, provided certain requirements are met. Other types of activities, such as the sale of a patient list to a marketing firm, would not be permitted under this rule without authorization from the individual. We do not believe that we can envision every possible disclosure of health information that would violate the privacy of an individual, so any list would be incomplete. Therefore, whether or not a particular activity is considered marketing, payment, treatment or health care operations will be a fact-based determination based on the activity's congruence with the particular definition.

Comment: Some industry groups stated that if an activity involves selling products, it is not disease management. They suggested we adopt a definition of disease management that differentiates use of information for the best interests of patient from uses undertaken for ''ulterior purposes'' such as advertising, marketing, or promoting separate products.

Response: We agree in general that the sale of unrelated products to individuals is not a population-based activity that supports treatment and payment. However, in certain circumstances marketing activities are permitted as a health care operation; see the definition of ''health care operations'' in § 164.501 and the related marketing requirements of § 164.514.

Comment: Some commenters complained that the absence of a definition for disease management created uncertainty, in view of the proposed rule's requirement to get authorization for marketing. They expressed concern that the effect would be to require patient consent for many activities that are desirable, not practicably done if authorization is required, and otherwise classifiable as treatment, payment, or health care operations. Examples provided include reminders for appointments, reminders to get preventive services like mammograms, and information about home management of chronic illnesses. They also stated that the proposed rule would prevent many disease management and preventive health activities.

Response: We agree that the distinction in the NPRM between disease management and marketing was unclear. Rather than provide a definition of disease management, this final rule defines marketing. We note that overlap between disease management and marketing exists today in practice and they cannot be distinguished easily with a definitional label. However, for purposes of this rule, the revised language makes clear for what activities an authorization is required. We note that under this rule many of the activities mentioned by commenters will not require authorizations under most circumstances. See the discussion of disease management under the definition of ''treatment'' in § 164.501.

Section 164.514(f)—Fundraising

Comment: Many comments objected to the requirement that an authorization from the individual be obtained for use and disclosure of protected health information for fundraising purposes. They argued that, in the case of not-for-profit health care providers, having to obtain authorization would be time consuming and costly, and that such a requirement would lead to a decrease in charitable giving. The commenters also urged that fundraising be included within the definition of health care operations. Numerous commenters suggested that they did not need unfettered access to patient information in order to carry out their fundraising campaigns. They stated that a limited data set restricted to name, address, and telephone number would be sufficient to meet their needs. Several commenters suggested that we create a voluntary opt-out provision so people can avoid solicitations.

Response: We agree with commenters that our proposal could have adversely effected charitable giving, and accordingly make several modifications to the proposal. First, the final rule allows a covered entity to use or disclose to a business associate protected health information without authorization to identify individuals for fundraising for its own benefit. Permissible fundraising activities include appeals for money, sponsorship of events, etc. They do not include royalties or remittances for the sale of products of third parties (except auctions, rummage sales, etc).

Second, the final rule allows a covered entity to disclose protected health information without authorization to an institutionally related foundation that has as its mission to benefit the covered entity. This special provision is necessary to accommodate tax code provisions which may not allow such foundations to be business associates of their associated covered entity.

We also agree that broad access to protected health information is unnecessary for fundraising and unnecessarily intrudes on individual privacy. The final rule limits protected health information to be used or disclosed for fundraising to demographic information and the date that treatment occurred. Demographic information is not defined in the rule, but will generally include in this context name, address and other contact information, age, gender, and insurance status. The term does not include any information about the illness or treatment.

We also agree that a voluntary opt-out is an appropriate protection, and require in § 164.520 that covered entities provide information on their fundraising activities in their ''Notice of Information Practices.'' As part of the notice and in any fundraising materials, covered entities must provide information explaining how individuals may opt out of fundraising communications.

Comment: Some commenters stated that use and disclosure of protected health information for fundraising, without authorization should be limited to not-for-profit entities. They suggested that not-for-profit entities were in greater need of charitable contributions and as such, they should be exempt from the authorization requirement while for-profit organizations should have to comply with the requirement.

Response: We do not agree that the profit status of a covered entity should determine its allowable use of protected health information for fundraising. Many for-profit entities provide the same services and have similar missions to not-for-profit entities. Therefore, the final rule does not make this distinction.

Comment: Several commenters suggested that the final rule should allow the internal use of protected health information for fundraising, without authorization, but not disclosure for fundraising. These commenters suggested that by limiting access of protected health information to only internal development offices concerns about misuse would be reduced.

Response: We do not agree. A number of commenters noted that they have related charitable foundations that raise funds for the covered entity, and we permit disclosures to such foundations to ensure that this rule does not interfere with charitable giving.

Comment: Several commenters asked us to address the content of fundraising letters. They pointed out that disease or condition-specific letters requesting contributions, if opened by the wrong person, could reveal personal information about the intended recipient.

Response: We agree that such communications raise privacy concerns. In the final rule, we limit the information that can be used or disclosed for fundraising, and exclude information about diagnosis, nature of services, or treatment.

Section 164.514(g)—Verification

Comment: A few commenters suggested that verification guidelines may need to be different as they apply to emergency clinical situations as opposed to routine data collection where delays do not threaten health.

Response: We agree, and make special provisions in §§ 164.510 and 164.512 for disclosures of protected health information by a covered entity without authorization where the individual is unable to agree or object to disclosure due to incapacity or other emergency circumstance.

For example, a health care provider may need to make disclosures to family members, close personal friends, and others involved in the individual's care in emergency situations. Similarly, a health care provider may need to respond to a request from a hospital seeking protected health information in

a circumstance described as an emergency. In each case, we require only that the covered entity exercise professional judgment, in the best interest of the patient, in deciding whether to make a disclosure. Based on the comments and our fact finding, this reflects current practice.

Comment: A few commenters stated the rules should include provisions for electronic verification of identity (such as Public Key Infrastructure (PKI)) as established in the regulations on Security and Electronic Signatures. One commenter suggested that some kind of PKI credentialing certificate should be required.

Response: This regulation does not address specific technical protocols utilized to meet the verification requirements. If the requirements of the rule are otherwise met, the mechanism for meeting them can be determined by the covered entity.

Comment: A few commenters wanted more clarification on the verification procedures. One commenter wanted to know if contract number is enough for verification. A few commenters wanted to know if a callback or authorization on a letterhead is acceptable. A few commenters wanted to know if plans are considered to ''routinely do business'' with all of their members.

Response: In the final rule, we modify the proposed provision and require covered entities to have policies and procedures reasonably designed to verify the identify and authority of persons requesting protected health information. Whether knowledge of a contract number is reasonable evidence of authority and identity will depend on the circumstances. Call-backs and letterhead are typically used today for verification, and are acceptable under this rule if reasonable under the circumstances. For communications with health plan members, the covered entity will already have information about each individual, collected during enrollment, that can be used to establish identity, especially for verbal or electronic inquiries. For example, today many health plans ask for the social security or policy number of individuals seeking information or assistance by telephone. How this verification is done is left up to the covered entity.

Comment: One commenter expressed the need for consistency on verification requirements between this rule and the Security regulation.

Response: We will make every effort to ensure consistency prior to publishing the final Security Rule.

Comment: One commenter stated that the verification language in proposed § 164.518(c)(2)(ii)(B)(1) would have created a presumption that ''a request for disclosure made by official legal process issued by a[n] administrative body'' is reasonable legal authority to disclose the protected health information. The commenter was concerned that this provision could be interpreted to permit a state agency to demand the disclosure of protected health information merely on the basis of a letter signed by an agency representative. The commenter believed that the rule specifically should defer to state or federal law on the disclosure of protected health information pursuant to legal process.

Response: The verification provisions in this rule are minimum requirements that covered entities must meet before disclosing protected health information under this regulation. They do not mandate disclosure, nor do they preempt state laws which impose additional restrictions on disclosure. Where state law regarding disclosures is more stringent, the covered entity must adhere to state law.

Comment: A few commenters wanted the verification requirements to apply to disclosures of protected health information for treatment, payment and operations purposes.

Response: We agree. This verification requirement applies to all disclosures of protected health information permitted by this rule, including for treatment, payment and operations, where the identity of the recipient is not known to the covered entity. Routine communications between providers, where existing relationships have been established, do not require special verification procedures.

Comment: A few commenters were concerned that a verbal inquiry for next of kin verification is not consistent with the verification guidelines of this verification subsection and that verbal inquiry would create problems because anyone who purports to be a next of kin could easily obtain information under false pretenses.

Response: In the final rule in § 164.514, we require the covered entity to verify the identity and authority of persons requesting protected health information, where the identity and authority of such person is not known to the covered entity. This applies to next of kin situations. Procedures for disclosures to next of kin, other family members and persons assisting in an individual's care are also discussed in § 164.510(b), which allows the covered entity to exercise professional judgment as to whether the disclosure is in the individual's best interest when the individual is not available to agree to the disclosure or is incapacitated. Requiring written proof of identity in many of these situations, such as when a family member is seeking to locate a relative in an emergency or disaster situation, would create enormous burden without a corresponding enhancement of privacy, and could cause unnecessary delays in these situations. We therefore believe that reliance on professional judgment provides a better framework for balancing the need for privacy with the need to locate and identify individuals.

Comment: A few commenters stated that the verification requirements will provide great uncertainty to providers who receive authorizations from life, disability income and long-term care insurers in the course of underwriting and claims investigation. They are unaware of any breaches of confidentiality associated with these circumstances and believe the rule creates a solution to a non-existent problem. Another commenter stated that it is too burdensome for health care providers to verify requests that are normally received verbally or via fax.

Response: This rule requires covered health care providers to adhere to current best practices for verification. That is, when the requester is not known to the covered provider, the provider makes a reasonable effort to determine that the protected health information is being sent to the entity authorized to receive it. Our fact finding reveals that this is often done by sending the information to a recognizable organizational address or if being transmitted by fax or phone by calling the requester back through the main organization switchboard rather than through a direct phone number. We agree that these procedures seem to work reasonably well in current practice and are sufficient to meet the relevant requirements in the final rule.

Comments: One comment suggested requiring a form of photo identification such as a driver's license or certain personal information such as date of birth to verify the identity of the individual.

Response: These are exactly the types of standard procedures for verifying the identity of individuals that are envisioned by the final rule. Most health care entities already conduct such procedures successfully. However, it is unwise to prescribe specific means of verification for all situations. Instead, we require policies and procedures reasonably designed for purposes of verification.

Comment: One professional association said that the example procedure described in the NPRM for asking questions to verify that an adult

acting for a young child had the requisite relationship to the child would be quite complex and difficult in practice. The comment asked for specific guidance as to what questions would constitute an adequate attempt to verify such a relationship.

Response: The final rule requires the covered entity to implement policies and procedures that are reasonably designed to comply with the verification requirement in § 164.514. It would not be possible to create the requested specific guidance which could deal with the infinite variety of situations that providers must face, especially the complex ones such as that described by the commenter. As with many of the requirements of this final rule, health care providers are given latitude and expected to make decisions regarding disclosures, based on their professional judgment and experience with common practice, in the best interest of the individual.

Comment: One commenter asserted that ascertaining whether a requestor has the appropriate legal authority is beyond the scope of the training or expertise of most employees in a physician's office. They believe that health care providers must be able to reasonably rely on the authority of the requestor.

Response: In the final regulation we require covered entities to have policies and procedures reasonably designed to verify the identify and authority of persons requesting health information. Where the requester is a public official and legal authority is at issue, we provide detailed descriptions of the acceptable methods for such verification in the final rule. For others, the covered entity must implement policies and procedures that are reasonably designed to comply with the requirement to verify the identity and authority of a requestor, but only if the requestor is unknown to the covered entity. As described above, we expect these policies and procedures to document currently used best practices and reliance on professional judgment in the best interest of the individual.

Comment: One commenter expressed concern that the verification/identification procedures may eliminate or significantly reduce their ability to utilize medical records copy services. As written, they believe the NPRM provides the latitude to set up copy service arrangements, but any change that would add restrictions would adversely affect their ability to process an individual's disability claim.

Response: The covered entity can establish reasonable policies and procedures to address verification in routine disclosures under business associate agreements, with, for example, medical records copy services. Nothing in the verification provisions would preclude those activities, nor have we significantly modified the NPRM provision on this issue.

Section 164.520—Notice of Privacy Practices for Protected Health Information

Comment: Many commenters supported the proposal to require covered entities to produce a notice of information practices. They stated that such notice would improve individuals' understanding of how their information may be used and disclosed and would help to build trust between individuals and covered entities. A few comments, however, argued that the notice requirement would be administratively burdensome and expensive without providing significant benefit to individuals.

Response: We retain the requirement for covered health care providers and health plans to produce a notice of information practices. We additionally require health care clearinghouses that create or receive protected health information other than as a business associate of another covered entity to produce a notice. We believe the notice will provide individuals with a clearer understanding of how their information may be used and disclosed and is essential to inform individuals of their privacy rights. The notice will focus individuals on privacy issues, and prompt individuals to have discussions about privacy issues with their health plans, health care providers, and other persons.

The importance of providing individuals with notice of the uses and disclosures of their information and of their rights with respect to that information is well supported by industry groups, and is recognized in current state and federal law. The July 1977 Report of the Privacy Protection Study Commission recommended that ''each medical-care provider be required to notify an individual on whom it maintains a medical record of the disclosures that may be made of information in the record without the individual's express authorization.'' [23] The Commission also recommended that ''an insurance institution * * * notify (an applicant or principal insured) as to: * * * the types of parties to whom and circumstances under which information about the individual may be disclosed without his authorization, and the types of information that may be disclosed; [and] * * * the procedures whereby the individual may correct, amend, delete, or dispute any resulting record about himself.'' [24] The Privacy Act (5 U.S.C. 552a) requires government agencies to provide notice of the routine uses of information the agency collects and the rights individuals have with respect to that information. In its report ''Best Principles for Health Privacy,'' the Health Privacy Working Group stated, ''Individuals should be given notice about the use and disclosure of their health information and their rights with regard to that information.'' [25] The National Association of Insurance Commissioners' Health Information Privacy Model Act requires carriers to provide a written notice of health information policies, standards, and procedures, including a description of the uses and disclosures prohibited and permitted by the Act, the procedures for authorizing and limiting disclosures and for revoking authorizations, and the procedures for accessing and amending protected health information.

Some states require additional notice. For example, Hawaii requires health care providers and health plans, among others, to produce a notice of confidentiality practices, including a description of the individual's privacy rights and a description of the uses and disclosures of protected health information permitted under state law without the individual's authorization. (HRS section 323C–13)

Today, health plan hand books and evidences of coverage include some of what is required to be in the notice. Industry and standard-setting organizations have also developed notice requirements. The National Committee for Quality Assurance accreditation guidelines state that an accredited managed care organization ''communicates to prospective members its policies and practices regarding the collection, use, and disclosure of medical information [and] * * * informs members * * * of its policies and procedures on * * * allowing members access to their medical records.'' [26] Standards of the American Society for Testing and Materials state,

[23] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 313.

[24] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 192.

[25] Health Privacy Working Group, ''Best Principles for Health Privacy,'' Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, July 1999, p.19.

[26] National Committee on Quality Assurance, ''Surveyor Guidelines for the Accreditation of MCOs,'' effective July 1, 2000—June 30, 2001, p. 324.

''Organizations and individuals who collect, process, handle, or maintain health information should provide individuals and the public with a notice of information practices.'' They recommend that the notice include, among other elements, ''a description of the rights of individuals, including the right to inspect and copy information and the right to seek amendments [and] a description of the types of uses and disclosures that are permitted or required by law without the individual's authorization.'' [27] We build on this well-established principle in this final rule.

Comment: We received many comments on the model notice provided in the proposed rule. Some commenters argued that patients seeing similar documents would be less likely to become disoriented when examining a new notice. Other commenters, however, opposed the inclusion of a model notice or expressed concern about particular language included in the model. They maintained that a uniform model notice would never capture the varying practices of covered entities. Many commenters opposed requirements for a particular format or specific language in the notice. They stated that covered entities should be afforded maximum flexibility in fashioning their notices. Other commenters requested inclusion of specific language as a header to indicate the importance of the notice. A few commenters recommended specific formatting requirements, such as font size or type.

Response: On the whole, we found commenters' arguments for flexibility in the regulation more persuasive than those arguing for more standardization. We agree that a uniform notice would not capture the wide variation in information practices across covered entities. We therefore do not include a model notice in the final rule, and do not require inclusion of specific language in the notice (except for a standard header). We also do not require particular formatting. We do, however, require the notice to be written in plain language. (See above for guidance on writing documents in plain language.) We also agree with commenters that the notice should contain a standard header to draw the individual's attention to the notice and facilitate the individual's ability to recognize the notice across covered entities.

We believe that post-publication guidance will be a more effective mechanism for helping covered entities design their notices than the regulation itself. After the rule is published, we can provide guidance on notice content and format tailored to different types of health plans and providers. We believe such specially designed guidance will be more useful than a one-size-fits-all model notice we might publish with this regulation.

Comment: Commenters suggested that the rule should require that the notice regarding privacy practices include specific provisions related to health information of unemancipated minors.

Response: Although we agree that minors and their parents should be made aware of practices related to confidentiality of protected health information of unemancipated minors, we do not require covered entities that treat minors or use their protected health information to include provisions in their notice that are not required of other covered entities. In general, the content of notice requirements in § 164.520(b) do not vary based on the status of the individual being served. We have decided to maintain consistency by declining to prescribe specific notice requirements for minors. The rule does permit a covered entity to provide individuals with notice of its policies and procedures with respect to anticipated uses and disclosures of protected health information (§ 164.520(b)(2)), and providers are encouraged to do so.

Comment: Some commenters argued that covered entities should not be required to distinguish between those uses and disclosures that are required by law and those that are permitted by law without authorization, because these distinctions may not always be clear and will vary across jurisdictions. Some commenters maintained that simply stating that the covered entity would make all disclosures required by law would be sufficient. Other comments suggested that covered entities should be able to produce very broadly stated notices so that repeated revisions and mailings of those revisions would not be necessary.

Response: While we believe that covered entities have an independent duty to understand the laws to which they are subject, we also recognize that it could be difficult to convey such legal distinctions clearly and concisely in a notice. We therefore eliminate the proposed requirement for covered entities to distinguish between those uses and disclosures that are required by and those that are permitted by law. We instead require that covered entities describe each purpose for which they are permitted or required to use or disclose protected health information under this rule and other applicable law without individual consent or authorization. Specifically, covered entities must describe the types of uses and disclosures they are permitted to make for treatment, payment, and health care operations. They must also describe each of the purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written consent or authorization (even if they do not plan to make a permissive use or disclosure). We believe this requirement provides individuals with sufficient information to understand how information about them can be used and disclosed and to prompt them to ask for additional information to obtain a clearer understanding, while minimizing covered entities' burden.

A notice that stated only that the covered entity would make all disclosures required by law, as suggested by some of these commenters, would fail to inform individuals of the uses and disclosures of information about them that are permitted, but not required, by law. We clarify that each and every disclosure required by law need not be listed on the notice. Rather, the covered entity can include a general statement that disclosures required by law will be made.

Comment: Some comments argued that the covered entity should not have to provide notice about uses and disclosures that are permitted under the rule without authorization. Other comments suggested that the notice should inform individuals about all of the uses and disclosures that may be made, with or without the individual's authorization.

Response: When the individual's permission is not required for uses and disclosures of information, we believe providing the required notice is the most effective means of ensuring that individuals are aware of how information about them may be shared. The notice need not describe uses and disclosures for which the individual's permission is required, because the individual will be informed of these at the time permission to use or disclose the information is requested.

We additionally require covered entities, even those required to obtain the individual's consent for use and disclosure of protected health information for treatment, payment, and health care operations, to describe those uses and disclosures in their notice. (See § 164.506 and the corresponding preamble discussion regarding consent requirements.) We require these uses

[27] ASTM, ''Standard Guide for Confidentiality, Privacy, Access and Data Security, Principles for Health Information Including Computer-Based Patient Records,'' E 1869–97, § 9.2.

and disclosures to be described in the notice in part in order to reduce the administrative burden on covered providers that are required to obtain consent. Rather than obtaining a new consent each time the covered provider's information policies and procedures are materially revised, covered providers may revise and redistribute their notice. We also expect that the description of how information may be used to carry out treatment, payment, and health care operations in the notice will be more detailed than in the more general consent document.

Comment: Some commenters argued that covered entities should not be required to provide notice of the right to request restrictions, because doing so would be burdensome to the covered entity and distracting to the individual; because individuals have the right whether they are informed of such right or not; and because the requirement would be unlikely to improve patient care.

Response: We disagree. We believe that the ability of an individual to request restrictions is an important privacy right and that informing people of their rights improves their ability to exercise those rights. We do not believe that adding a sentence to the notice is burdensome to covered entities.

Comment: We received comments supporting inclusion of a contact point in the notice, so that individuals will not be forced to make multiple calls to find someone who can assist them with the issues in the notice.

Response: We retain the requirement, but clarify that the title of the contact person is sufficient. A person's name is not required.

Comment: Some commenters argued that we could facilitate compliance by requiring the notice to include the proposed requirement that covered entities use and disclose only the minimum necessary protected health information.

Response: We do not agree that adding such a requirement would strengthen the notice. The purpose of the notice is to inform individuals of their privacy rights, and of the purposes for which protected health information about them may be used or disclosed. Informing individuals that covered entities may use and disclose only the minimum necessary protected health information for a purpose would not increase individuals' understanding of their rights or the purposes for which information may be used or disclosed.

Comment: A few commenters supported allowing covered entities to apply changes in their information practices to protected health information obtained prior to the change. They argued that requiring different protections for information obtained at different times would be inefficient and extremely difficult to administer. Some comments supported requiring covered entities to state in the notice that the information policies and procedures are subject to change.

Response: We agree. In the final rule, we provide a mechanism by which covered entities may revise their privacy practices and apply those revisions to protected health information they already maintain. We permit, but do not require, covered entities to reserve the right to change their practices and apply the revised practices to information previously created or obtained. If a covered entity wishes to reserve this right, it must make a statement to that effect in its notice. If it does not make such a statement, the covered entity may still revise its privacy practices, but it may apply the revised practices only to protected health information created or obtained after the effective date of the notice in which the revised practices are reflected. See § 164.530(i) and the corresponding preamble discussion of requirements regarding changes to information policies and procedures.

Comment: Some commenters requested clarification of the term ''material changes'' so that entities will be comfortable that they act properly after making changes to their information practices. Some comments stated that entities should notify individuals whenever a new category of disclosures to be made without authorization is created.

Response: The concept of ''material change'' appears in other notice laws, such as the ERISA requirements for summary plan descriptions. We therefore retain the ''materiality'' condition for revision of notices, and encourage covered entities to draw on the concept as it has developed through those other laws. We agree that the addition of a new category of use or disclosure of health information that may be made without authorization would likely qualify as a material change.

Comment: We proposed to permit covered entities to implement revised policies and procedures without first revising the notice if a compelling reason existed to do so. Some commenters objected to this proposal because they were concerned that the ''compelling reason'' exception would give covered entities broad discretion to engage in post hoc violations of its own information practices.

Response: We agree and eliminate this provision. Covered entities may not implement revised information policies and procedures before properly documenting the revisions and updating their notice. See § 164.530(i). Because in the final rule we require the notice to include all disclosures that may be made, not only those the covered entity intends to make, we no longer need this provision to accommodate emergencies.

Comment: Some comments suggested that we require covered entities to maintain a log of all past notices, with changes from the previous notice highlighted. They further suggested we require covered entities to post this log on their web sites.

Response: In accordance with § 164.530(j)(2), a covered entity must retain for six years a copy of each notice it issues. We do not require highlighting of changes to the notice or posting of prior notices, due to the associated administrative burdens and the complexity such a requirement would build into the notice over time. We encourage covered entities, however, to make such materials available upon request.

Comment: Several commenters requested clarification about when, relative to the compliance date, covered entities are required to produce their notice. One commenter suggested that covered entities be allowed a period not less than 180 days after adoption of the final rule to develop and distribute the notice. Other comments requested that the notice compliance date be consistent with other HIPAA regulations.

Response: We require covered entities to have a notice available upon request as of the compliance date of this rule (or the compliance date of the covered entity if such date is later). See § 164.534 and the corresponding preamble discussion of the compliance date.

Comment: Some commenters suggested that covered entities, particularly covered health care providers, should be required to discuss the notice with individuals. They argued that posting a notice or otherwise providing the notice in writing may not achieve the goal of informing individuals of how their information will be handled, because some individuals may not be literate or able to function at the reading level used in the notice. Others argued that entities should have the flexibility to choose alternative modes of communicating the information in the notice, including voice disclosure. In contrast, some commenters were concerned that requirements to provide the notice in plain language or in languages other than English would be overly burdensome.

Response: We require covered entities to write the notice in plain language so that the average reader will be able to understand the notice. We encourage, but do not require, covered entities to consider alternative means of communicating with certain populations. We note that any covered entity that is a recipient of federal financial assistance is generally obligated under Title VI of the Civil Rights Act of 1964 to provide material ordinarily distributed to the public in the primary languages of persons with limited English proficiency in the recipients' service areas. While we believe the notice will prompt individuals to initiate discussions with their health plans and health care providers about the use and disclosure of health information, we believe this should be a matter left to each individual and that requiring covered entities to initiate discussions with each individual would be overly burdensome.

Comment: Some commenters suggested that covered entities, particularly health plans, should be permitted to distribute their notice in a newsletter or other communication with individuals.

Response: We agree, so long as the notice is sufficiently separate from other important documents. We therefore prohibit covered entities from combining the notice in a single document with either a consent (§ 164.506) or an authorization (§ 164.508), but do not otherwise prohibit covered entities from including the notice in or with other documents the covered entity shares with individuals.

Comment: Some comments suggested that covered entities should not be required to respond to requests for the notice from the general public. These comments indicated that the requirement would place an undue burden on covered entities without benefitting individuals.

Response: We proposed that the notice be publicly available so that individuals may use the notice to compare covered entities' privacy practices and to select a health plan or health care provider accordingly. We therefore retain the proposed requirement for covered entities to provide the notice to any person who requests a copy, including members of the general public.

Comment: Many commenters argued that the distribution requirements for health plans should be less burdensome. Some suggested requiring distribution upon material revision, but not every three years. Some suggested that health plans should only be required to distribute their notice annually or upon re-enrollment. Some suggested that health plans should only have to distribute their notice upon initial enrollment, not re-enrollment. Other commenters supported the proposed approach.

Response: We agree that the notice distribution requirements for health plans can be less burdensome than in the NPRM while still being effective. In the final rule, we reduce health plans' distribution burden in several ways. First, we require health plans to remind individuals every three years of the availability of the notice and of how to obtain a copy of the notice, rather than requiring the notice to be distributed every three years as proposed. Second, we clarify that health plans only have to distribute the notice to new enrollees on enrollment, not to current members of the health plan upon re-enrollment. Third, we specifically allow all covered entities to distribute the notice electronically in accordance with § 164.520(c)(3).

We retain the requirement for health plans to distribute the notice within 60 days of a material revision. We believe the revised distribution requirements will ensure that individuals are adequately informed of health plans' information practices and any changes to those procedures, without unduly burdening health plans.

Comment: Many commenters argued that health plans should not be required to distribute their notice to every person covered by the plan. They argued that distributing the notice to every family member would be unnecessarily duplicative, costly, and difficult to administer. They suggested that health plans only be required to distribute the notice to the primary participant or to each household with one or more insured individuals.

Response: We agree, and clarify in the final rule that a health plan may satisfy the distribution requirement by providing the notice to the named insured on behalf of the dependents of that named insured. For example, a group health plan may satisfy its notice requirement by providing a single notice to each covered employee of the plan sponsor. We do not require the group health plan to distribute the notice to each covered employee and to each covered dependent of those employees.

Comment: Many comments requested clarification about health plans' ability to distribute the notice via other entities. Some commenters suggested that group health plans should be able to satisfy the distribution requirement by providing copies of the notice to plan sponsors for delivery to employees. Others requested clarification that covered health care providers are only required to distribute their own notice and that health plans should be prohibited from using their affiliated providers to distribute the health plan's notice.

Response: We require health plans to distribute their notice to individuals covered by the health plan. Health plans may elect to hire or otherwise arrange for others, including group health plan sponsors and health care providers affiliated with the health plan, to carry out this distribution. We require covered providers to distribute only their own notices, and neither require nor prohibit health plans and health care providers from devising whatever arrangements they find suitable to meet the requirements of this rule. However, if a covered entity arranges for another person or entity to distribute the covered entity's notice on its behalf and individuals do not receive such notice, the covered entity would be in violation of the rule.

Comment: Some comments stated that covered providers without direct patient contact, such as clinical laboratories, might not have sufficient patient contact information to be able to mail the notice. They suggested we require or allow such providers to form agreements with referring providers or other entities to distribute notices on their behalf or to include their practices in the referring entity's own notice.

Response: We agree with commenters' concerns about the potential administrative and financial burdens of requiring covered providers that have indirect treatment relationships with individuals, such as clinical laboratories, to distribute the notice. Therefore, we require these covered providers to provide the notice only upon request. In addition, these covered providers may elect to reach agreements with other entities distribute their notice on their behalf, or to participate in an organized health care arrangement that produces a joint notice. See § 164.520(d) and the corresponding preamble discussion of joint notice requirements.

Comment: Some commenters requested that covered health care providers be permitted to distribute their notice prior to an individual's initial visit so that patients could review the information in advance of the visit. They suggested that distribution in advance would reduce the amount of time covered health care providers' staff would have to spend explaining the notice to patients in the office. Other comments argued that providers should

distribute their notice to patients at the time the individual visits the provider, because providers lack the administrative infrastructure necessary to develop and distribute mass communications and generally have difficulty identifying active patients.

Response: In the final rule, we clarify that covered providers with direct treatment relationships must provide the notice to patients no later than the first service delivery to the patient after the compliance date. For the reasons identified by these commenters, we do not require covered providers to send their notice to the patient in advance of the patient's visit. We do not prohibit distribution in advance, but only require distribution to the patient as of the time of the visit. We believe this flexibility will allow each covered provider to develop procedures that best meet its and its patients' needs.

Comment: Some comments suggested that covered providers should be required to distribute the notice as of the compliance date. They noted that if the covered provider waited to distribute the notice until first service delivery, it would be possible (pursuant to the rule) for a use or disclosure to be made without the individual's authorization, but before the individual receives the notice.

Response: Because health care providers generally lack the administrative infrastructure necessary to develop and distribute mass communications and generally have difficulty identifying active patients, we do not require covered providers to distribute the notice until the first service delivery after the compliance date. We acknowledge that this policy allows uses and disclosure of health information without individuals' consent or authorization before the individual receives the notice. We require covered entities, including covered providers, to have the notice available upon request as of the compliance date of the rule. Individuals may request a copy of the notice from their provider at any time.

Comment: Many commenters were concerned with the requirement that covered providers post their notice. Some commenters suggested that covered hospital-based providers should be able to satisfy the distribution requirements by posting their notice in multiple locations at the hospital, rather than handing the notice to patients—particularly with respect to distribution after material revisions have been made. Some additionally suggested that these covered providers should have copies of the notice available on site. Some commenters emphasized that the notice must be clear and conspicuous to give individuals meaningful and effective notice of their rights. Other commenters noted that posting the notice will not inform former patients who no longer see the provider.

Response: We clarify in the final rule that the requirement to post a notice does not substitute for the requirement to give individuals a notice or make notices available upon request. Covered providers with direct treatment relationships, including covered hospitals, must give a copy of the notice to the individual as of first service delivery after the compliance date. After giving the individual a copy of the notice as of that first visit, the covered provider has no other obligation to actively distribute the notice. We believe it is unnecessarily burdensome to require covered providers to mail the notice to all current and former patients each time the notice is revised, because unlike health plans, providers may have a difficult time identifying active patients. All individuals, including those who no longer see the covered provider, have the right to receive a copy of the notice on request.

If the covered provider maintains a physical delivery site, it must also post the notice (including revisions to the notice) in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered provider to be able to read the notice. The covered provider must also have the notice available on site for individuals to be able to request and take with them.

Comment: Some comments requested clarification about the distribution requirements for a covered entity that is a health plan and a covered health care provider.

Response: Under § 164.504(g), discussed above, covered entities that conduct multiple types of covered functions, such as the kind of entities described in the above comments, are required to comply with the provisions applicable to a particular type of health care function when acting in that capacity. Thus, in the example described above, the covered entity is required by § 164.504(g) to follow the requirements for health plans with respect to its actions as a health plan and to follow the requirements for health care providers with respect to its actions as a health care provider.

Comment: We received many comments about the ability of covered entities to distribute their notices electronically. Many commenters suggested that we permit covered entities to distribute the notice electronically, either via a web site or e-mail. They argued that covered entities are increasingly using electronic technology to communicate with patients and otherwise administer benefits. They also noted that other regulations permit similar documents, such as ERISA-required summary plan descriptions, to be delivered electronically. Some commenters suggested that electronic distribution should be permitted unless the individual specifically requests a hard copy or lacks electronic access. Some argued that entities should be able to choose a least-cost alternative that allows for periodic changes without excessive mailing costs. A few commenters suggested requiring covered entities to distribute notices electronically.

Response: We clarify in the final rule that covered entities may elect to distribute their notice electronically, provided the individual agrees to receiving the notice electronically and has not withdrawn such agreement. We do not require any particular form of agreement. For example, a covered provider could ask an individual at the time the individual requests a copy of the notice whether she prefers to receive it in hard copy or electronic form. A health plan could ask an individual applying for coverage to provide an e-mail address where the health plan can send the individual information. If the individual provides an e-mail address, the health plan can infer agreement to obtain information electronically.

An individual who has agreed to receive the notice electronically, however, retains the right to request a hard copy of the notice. This right must be described in the notice. In addition, if the covered entity knows that electronic transmission of the notice has failed, the covered entity must produce a hard copy of the notice. We believe this provision allows covered entities flexibility to provide the notice in the form that best meets their needs without compromising individuals' right to adequate notice of covered entities' information practices.

We note that covered entities may also be subject to the Electronic Signatures in Global and National Commerce Act. This rule is not intended to alter covered entities' requirements under that Act.

Comment: Some commenters were concerned that covered providers with ''face-to-face'' patient contact would have a competitive disadvantage against covered internet-based providers, because the face-to-face providers would be required to distribute the notice in hard copy while internet-based providers could satisfy the requirement

by requiring review of the notice on the web site before processing an order. They suggested allowing face-to-face covered providers to satisfy the distribution requirement by asking patients to review the notice posted on site.

Response: We clarify in the final rule that covered health care providers that provide services to individuals over the internet have direct treatment relationships with those individuals. Covered internet-based providers, therefore, must distribute the notice at the first service delivery after the compliance date by automatically and contemporaneously providing the notice electronically in response to the individual's first request for service, provided the individual agrees to receiving the notice electronically.

Even though we require all covered entity web sites to post the entity's notice prominently, we note that such posting is not sufficient to meet the distribution requirements. A covered internet-based provider must send the notice electronically at the individual's first request for service, just as other covered providers with direct treatment relationships must give individuals a copy of the notice as of the first service delivery after the compliance date.

We do not intend to create competitive advantages among covered providers. A web-based and a non-web-based covered provider each have the same alternatives available for distribution of the notice. Both types of covered providers may provide either a paper copy or an electronic copy of the notice.

Comment: We received several comments suggesting that some covered entities should be exempted from the notice requirement or permitted to combine notices with other covered entities. Many comments argued that the notice requirement would be burdensome for hospital-based physicians and result in numerous, duplicative notices that would be meaningless or confusing to patients. Other comments suggested that multiple health plans offered through the same employer should be permitted to produce a single notice.

Response: We retain the requirement for all covered health care providers and health plans to produce a notice of information practices. Health care clearinghouses are required to produce a notice of information practices only to the extent the clearinghouse creates or receives protected health information other than as a business associate of a covered entity. See § 164.500(b)(2). Two other types of covered entities are not required to produce a notice: a correctional institution that is a covered entity and a group health plan that provides benefits only through one or more contracts of insurance with health insurance issuers or HMOs.

We clarify in § 164.504(d), however, that affiliated covered entities under common ownership or control may designate themselves as a single covered entity for purposes of this rule. An affiliated covered entity is only required to produce a single notice.

In addition, covered entities that participate in an organized health care arrangement—which could include hospitals and their associated physicians—may choose to produce a single, joint notice, if certain requirements are met. See § 164.501 and the corresponding preamble discussion of organized health care arrangements.

We clarify that each covered entity included in a joint notice must meet the applicable distribution requirements. If any one of the covered entities, however, provides the notice to a given individual, the distribution requirement with respect to that individual is met for all of the covered entities included in the joint notice. For example, a covered hospital and its attending physicians may elect to produce a joint notice. When an individual is first seen at the hospital, the hospital must provide the individual with a copy of the joint notice. Once the hospital has done so, the notice distribution requirement for all of the attending physicians that provide treatment to the individual at the hospital and that are included in the joint notice is satisfied.

Comment: We solicited and received comments on whether to require covered entities to obtain the individual's signature on the notice. Some commenters suggested that requiring a signature would convey the importance of the notice, would make it more likely that individuals read the notice, and could have some of the same benefits of a consent. They noted that at least one state already requires entities to make a reasonable effort to obtain a signed notice. Other comments noted that the signature would be useful for compliance and risk management purposes because it would document that the individual had received the notice.

The majority of commenters on this topic, however, argued that a signed acknowledgment would be administratively burdensome, inconsistent with the intent of the Administrative Simplification requirements of HIPAA, impossible to achieve for incapacitated individuals, difficult to achieve for covered entities that do not have direct contact with patients, inconsistent with other notice requirements under other laws, misleading to individuals who might interpret their signature as an agreement, inimical to the concept of permitting uses and disclosures without authorization, and an insufficient substitute for authorization.

Response: We agree with the majority of commenters and do not require covered entities to obtain the individual's signed acknowledgment of receipt of the notice. We believe that we satisfied most of the arguments in support of requiring a signature with the new policy requiring covered health care providers with direct treatment relationships to obtain a consent for uses and disclosures of protected health information to carry out treatment, payment, and health care operations. See § 164.506 and the corresponding preamble discussion of consent requirements. We note that this rule does not preempt other applicable laws that require a signed notice and does not prohibit a covered entity from requesting an individual to sign the notice.

Comment: Some commenters supported requiring covered entities to adhere to their privacy practices, as described in their notice. They argued that the notice is meaningless if a covered entity does not actually have to follow the practices contained in its notice. Other commenters were concerned that the rule would prevent a covered entity from using or disclosing protected health information in otherwise lawful and legitimate ways because of an intentional or inadvertent omission from its published notice. Some of these commenters suggested requiring the notice to include a description of some or all disclosures that are required or permitted by law. Some commenters stated that the adherence requirement should be eliminated because it would generally inhibit covered entities' ability to innovate and would be burdensome.

Response: We agree that the value of the notice would be significantly diminished absent a requirement that covered entities adhere to the statements they make in their notices. We therefore retain the requirement for covered entities to adhere to the terms of the notice. See § 164.502(i).

Many of these commenters' concerns regarding a covered entity's inability to use or disclose protected health information due to an intentional or inadvertent omission from the notice are addressed in our revisions to the proposed content requirements for the notice. Rather than require covered entities to describe only those uses and

disclosures they anticipate making, as proposed, we require covered entities to describe all uses and disclosures they are required or permitted to make under the rule without the individual's consent or authorization. We permit a covered entity to provide a statement that it will disclose protected health information that is otherwise required by law, as permitted in § 164.512(a), without requiring them to list all state laws that may require disclosure. Because the notice must describe all legally permissible uses and disclosures, the notice will not generally preclude covered entities from making any uses or disclosures they could otherwise make without individual consent or authorization. This change will also ensure that individuals are aware of all possible uses and disclosures that may occur without their consent or authorization, regardless of the covered entity's current practices.

We encourage covered entities, however, to additionally describe the more limited uses and disclosures they actually anticipate making in order to give individuals a more accurate understanding of how information about them will be shared. We expect that certain covered entities will want to distinguish themselves on the basis of their privacy protections. We note that a covered entity that chooses to exercise this option must clearly state that, at a minimum, the covered entity may make disclosures that are required by law and that are necessary to avert a serious and imminent threat to health or safety.

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

Section 164.522(a)—Right of an Individual To Request Restriction of Uses and Disclosures

Comment: Several commenters supported the language in the NPRM regarding the right to request restrictions. One commenter specifically stated that this is a balanced approach that addresses the needs of the few who would have reason to restrict disclosures without negatively affecting the majority of individuals. At least one commenter explained that if we required consent or authorization for use and disclosure of protected health information for treatment, payment, and health care operations then we must also have a right to request restrictions of such disclosure in order to make the consent meaningful.

Many commenters requested that we delete this provision, claiming it would interfere with patient care, payment, and data integrity. Most of the commenters that presented this position asserted that the framework of giving patients control over the use or disclosure of their information is contrary to good patient care because incomplete medical records may lead to medical errors, misdiagnoses, or inappropriate treatment decisions. Other commenters asserted that covered entities need complete data sets on the populations they serve to effectively conduct research and quality improvement projects and that restrictions would hinder research, skew findings, impede quality improvement, and compromise accreditation and performance measurement.

Response: We acknowledge that widespread restrictions on the use and disclosure of protected health information could result in some difficulties related to payment, research, quality assurance, etc. However, in our efforts to protect the privacy of health information about individuals, we have sought a balance in determining the appropriate level of individual control and the smooth operation of the health care system. In the final rule, we require certain covered providers and permit all covered entities to obtain consent from individuals for use and disclosure of protected health information for treatment, payment, and health care operations (see § 164.506). In order to give individuals some control over their health information for uses and disclosures of protected health information for treatment, payment, and health care operations, we provide individuals with the opportunity to request restrictions of such uses and disclosures.

Because the right to request restrictions encourages discussions about how protected health information may be used and disclosed and about an individual's concerns about such uses and disclosures, it may improve communications between a provider and patient and thereby improve care. According to a 1999 survey on the Confidentiality of Medical Records by the California HealthCare Foundation, one out of every six people engage in behavior to protect themselves from unwanted disclosures of health information, such as lying to providers or avoiding seeking care. This indicates that, without the ability to request restrictions, individuals would have incentives to remain silent about important health information that could have an effect on their health and health care, rather than consulting a health care provider.

Further, this policy is not a dramatic change from the status quo. Today, many state laws restrict disclosures for certain types of health information without patient's authorization. Even if there is no mandated requirement to restrict disclosures of health information, providers may agree to requests for restrictions of disclosures when a patient expresses particular sensitivity and concern for the disclosure of health information.

We agree that there may be instances in which a restriction could negatively affect patient care. Therefore, we include protections against this occurrence. First, the right to request restrictions is a right of individuals to make the request. A covered entity may refuse to restrict uses and disclosures or may agree only to certain aspects of the individual's request if there is concern for the quality of patient care in the future. For example, if a covered provider believes that it is not in the patient's best medical interest to have such a restriction, the provider may discuss the request for restriction with the patient and give the patient the opportunity to explain the concern for disclosure. Also, a covered provider who is concerned about the implications on future treatment can agree to use and disclose sensitive protected health information for treatment purposes only and agree not to disclose information for payment and operation purposes. Second, a covered provider need not comply with a restriction that has been agreed to if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment. This exception should limit the harm to health that may otherwise result from restricting the use or disclosure of protected health information. We encourage covered providers to discuss with individuals that the information may be used or disclosed in emergencies. We require that the covered entity that discloses restricted protected health information in an emergency request that the health care provider that receives such information not further use or re-disclose the information.

Comment: Some health plans stated that an institutionalized right to restrict can interfere with proper payment and can make it easier for unscrupulous providers or patients to commit fraud on insurance plans. They were concerned that individuals could enter into restrictions with providers to withhold information to insurance companies so that the insurance company would not know about certain conditions when underwriting a policy.

Response: This rule does not enhance the ability of unscrupulous patients or health care providers to engage in deceptive or fraudulent withholding of information. This rule grants a right to request a restriction, not an absolute right to restrict. Individuals can make such requests today. Other laws criminalize insurance fraud; this regulation does not change those laws.

Comment: One commenter asserted that patients cannot anticipate the significance that one aspect of their medical information will have on treatment of other medical conditions, and therefore, allowing them to restrict use or disclosure of some information is contrary to the patient's best interest.

Response: We agree that patients may find it difficult to make such a calculus, and that it is incumbent on health care providers to help them do so. Health care providers may deny requests for or limit the scope of the restriction requested if they believe the restriction is not in the patient's best interest.

Comment: One commenter asked whether an individual's restriction to disclosure of information will be a bar to liability for misdiagnosis or failure to diagnose by a covered entity who can trace its error back to the lack of information resulting from such restriction.

Response: Decisions regarding liability and professional standards are determined by state and other law. This rule does not establish or limit liability for covered entities under those laws. We expect that the individual's request to restrict the disclosure of their protected health information would be considered in the decision of whether or not a covered entity is liable.

Comment: One commenter requested that we allow health plans to deny coverage or reimbursement when a covered health care provider's agreement to restrict use or disclosure prevents the plan from getting the information that is necessary to determine eligibility or coverage.

Response: In this rule, we do not modify insurers' rules regarding information necessary for payment. We recognize that restricting the disclosure of information may result in a denial of payment. We expect covered providers to explain this possibility to individuals when considering their requests for restrictions and to make alternative payment arrangements with individuals if necessary.

Comment: Some commenters discussed the administrative burden and cost of the requirement that individuals have the right to request restrictions and that trying to segregate certain portions of information for protection may be impossible. Others stated that the administrative burden would make providers unable to accommodate restrictions, and would therefore give patients false expectations that their right to request restrictions may be acted upon. One commenter expressed concern that large covered providers would have a particularly difficult time establishing a policy whereby the covered entity could agree to restrictions and would have an even more difficult time implementing the restrictions since records may be kept in multiple locations and accessed by multiple people within the organization. Still other commenters believed that the right to request restrictions would invite argument, delay, and litigation.

Response: We do not believe that this requirement is a significant change from current practice. Providers already respond to requests by patients regarding sensitive information, and are subject to state law requirements not to disclose certain types of information without authorization. This right to request is permissive so that covered entities can balance the needs of particular individuals with the entity's ability to manage specific accommodations.

Comment: Some commenters were concerned that a covered entity would agree to a restriction and then realize later that the information must be disclosed to another caregiver for important medical care purposes.

Response: Some individuals seek treatment only on the condition that information about that treatment will not be shared with others. We believe it is necessary and appropriate, therefore, that when a covered provider agrees to such a restriction, the individual must be able to rely on that promise. We strongly encourage covered providers to consider future treatment implications of agreeing to a restriction. We encourage covered entities to inform others of the existence of a restriction when appropriate, provided that such notice does not amount to a *de facto* disclosure of the restricted information. If the covered provider subject to the restriction believes that disclosing the protected health information that was created or obtained subject to the restriction is necessary to avert harm (and it is not for emergency treatment), the provider must ask the individual for permission to terminate or modify the restriction. If the individual agrees to the termination of the restriction, the provider must document this termination by noting this agreement in the medical record or by obtaining a written agreement of termination from the individual and may use or disclose the information for treatment. If the individual does not agree to terminate or modify the restriction, however, the provider must continue to honor the restriction with respect to protected health information that was created or received subject to the restriction. We note that if the restricted protected health information is needed to provide emergency treatment to the individual who requested the restriction, the covered entity may use or disclose such information for such treatment.

Comment: Commenters asked that we require covered entities to keep an accounting of the requests for restrictions and to report this information to the Department in order for the Department to determine whether covered entities are showing ''good faith'' in dealing with these requests.

Response: We require that covered entities that agree to restrictions with individuals document such restrictions. A covered entity must retain such documentation for six years from the date of its creation or the date when it last was in effect, whichever is later. We do not require covered entities to keep a record of all requests made, including those not agreed to, nor that they report such requests to the Department. The decision to agree to restrictions is that of the covered entity. Because there is no requirement to agree to a restriction, there is no reason to impose the burden to document requests that are denied. Any reporting requirement could undermine the purpose of this provision by causing the sharing, or appearance of sharing, of information for which individuals are seeking extra protection.

Comment: One commenter asserted that providers that currently allow such restrictions will choose not to do so under the rule based on the guidance of legal counsel and loss prevention managers, and suggested that the Secretary promote competition among providers with respect to privacy by developing a third-party ranking mechanism.

Response: We believe that providers will do what is best for their patients, in accordance with their ethics codes, and will continue to find ways to accommodate requested restrictions when they believe that it is in the patients' best interests. We anticipate that providers who find such action to be of commercial benefit will notify consumers of their willingness to be responsive to such requests. Involving third parties could undermine the purpose of this provision, by causing the sharing, or appearance of sharing, of information for which individuals are seeking extra protection.

Comment: One commenter said that any agreement regarding patient-requested restrictions should be in writing before a covered provider would be held to standards for compliance.

Response: We agree that agreed to restrictions must be documented in writing, and we require that covered entities that agree to restrictions document those restrictions in accordance with § 164.530(j). The writing need not be formal; a notation in the medical record will suffice. We disagree with the request that an agreed to restriction be reduced to writing in order to be enforced. If we adopted the requested policy, a covered entity could agree to a restriction with an individual, but avoid being held to this agreed to restriction under the rule by failing to document the restriction. This would give a covered entity the opportunity to agree to a restriction and then, at its sole discretion, determine if it is enforceable by deciding whether or not to make a note of the restriction in the record about the individual. Because the covered entity has the ability to agree or fail to agree to a restriction, we believe that once the restriction is agreed to, the covered entity must honor the agreement. Any other result would be deceptive to the individual and could lead an individual to disclose health information under the assumption that the uses and disclosures will be restricted. Under § 164.522, a covered entity could be found to be in violation of the rule if it fails to put an agreed-upon restriction in writing and also if it uses or discloses protected health information inconsistent with the restriction.

Comment: Some commenters said that the right to request restrictions should be extended to some of the uses and disclosures permitted without authorization in § 164.510 of the NPRM, such as disclosures to next of kin, for judicial and administrative proceedings, for law enforcement, and for governmental health data systems. Other commenters said that these uses and disclosures should be preserved without an opportunity for individuals to opt out.

Response: We have not extended the right to request restrictions under this rule to disclosures permitted in § 164.512 of the final rule. However, we do not preempt other law that would enforce such agreed-upon restrictions. As discussed in more detail, above, we have extended the right to request restrictions to disclosures to persons assisting in the individual's care, such as next of kin, under § 164.510(b). Any restriction that a covered entity agrees to with respect to persons assisting in the individual's care in accordance with the rule will be enforceable under the rule.

Comment: A few commenters raised the question of the effect of a restriction agreed to by one covered entity that is part of a larger covered entity, particularly a hospital. Commenters were also concerned about who may speak on behalf of the covered entity.

Response: All covered entities are required to establish policies and procedures for providing individuals the right to request restrictions, including policies for who may agree to such restrictions on the covered entity's behalf. Hospitals and other large entities that are concerned about employees agreeing to restrictions on behalf of the organization will have to make sure that their policies are communicated appropriately to those employees. The circumstances under which members of a covered entity's workforce can bind the covered entity are a function of other law, not of this regulation.

Comment: Commenters expressed confusion about the intended effect of any agreed-upon restrictions on downstream covered entities. They asserted that it would be extremely difficult for a requested restriction to be followed through the health care system and that it would be unfair to hold covered entities to a restriction when they did not agree to such restriction. Specifically, commenters asked whether a covered provider that receives protected health information in compliance with this rule from a physician or medical group that has agreed to limit certain uses of the information must comply with the original restriction. Other commenters expressed concern that not applying a restriction to downstream covered entities is a loophole and that all downstream covered providers and health plans should be bound by the restrictions.

Response: Under the final rule, a restriction that is agreed to between an individual and a covered entity is only binding on the covered entity that agreed to the restriction and not on downstream entities. It would also be binding on any business associate of the covered entity since a business associate can not use or disclose protected health information in any manner that a covered entity would not be permitted to use or disclose such information. We realize that this may limit the ability of an individual to successfully restrict a use or disclosure under all circumstances, but we take this approach for two reasons. First, we allow covered entities to refuse individuals' requests for restrictions. Requiring downstream covered entities to abide by a restriction would be tantamount to forcing them to agree to a request to which they otherwise may not have agreed. Second, some covered entities have information systems which will allow them to accommodate such requests, while others do not. If the downstream provider is in the latter category, the administrative burden of such a requirement would be unmanageable.

We encourage covered entities to explain this limitation to individuals when they agree to restrictions, so individuals will understand that they need to ask all their health plans and providers for desired restrictions. We also require that a covered entity that discloses protected health information to a health care provider for emergency treatment, in accordance with § 164.522 (a)(iii), to request that the recipient not further use or disclose the information.

Comment: One commenter requested that agreed-to restrictions of a covered entity not be applied to business associates.

Response: As stated in § 164.504(e)(2), business associates are acting on behalf of, or performing services for, the covered entity and may not, with two narrow exceptions, use or disclose protected health information in a manner that would violate this rule if done by the covered entity. Business associates are agents of the covered entity with respect to protected health information they obtain through the business relationship. If the covered entity agrees to a restriction and, therefore, is bound to such restriction, the business associate will also be required to comply with the restriction. If the covered entity has agreed to a restriction, the satisfactory assurances from the business associate, as required in § 164.504(e), must include assurances that protected health information will not be used or disclosed in violation of an agreed to restriction.

Comment: One commenter requested clarification that the right to request restrictions cannot be used to restrict the creation of de-identified information.

Response: We found no reason to treat the use of protected health information to create de-identified information different from other uses of protected health information. The right to request restriction applies to any use or disclosure of protected health information to carry out treatment, payment, or health care operations. If the covered entity uses protected health information to create de-identified information, the covered entity need not agree to a restriction of this use.

Comment: Some commenters stated that individuals should be given a true right to restrict uses and disclosures of protected health information in certain defined circumstances (such as for sensitive information) rather than a right to request restrictions.

Response: We are concerned that a right to restrict could create conflicts with the professional ethical obligations of providers and others. We believe it is better policy to allow covered entities to refuse to honor restrictions that they believe are not appropriate and leave the individual with the option of seeking service from a different covered entity. In addition, many covered entities have information systems that would make it difficult or impossible to accommodate certain restrictions.

Comment: Some commenters requested that self-pay patients have additional rights to restrict protected health information. Others believed that this policy would result in de facto discrimination against those patients that could not afford to pay out-of-pocket.

Response: Under the final rule, the decision whether to tie an agreement to restrict to the way the individual pays for services is left to each covered entity. We have not provided self-pay patients with any special rights under the rule.

Comment: Some commenters suggested that we require restrictions to be clearly noted so that insurers and other providers would be aware that they were not being provided with complete information.

Response: Under the final rule, we do not require or prohibit a covered entity to note the existence of an omission of information. We encourage covered entities to inform others of the existence of a restriction, in accordance with professional practice and ethics, when appropriate to do so. In deciding whether or not to disclose the existence of a restriction, we encourage the covered entity to carefully consider whether disclosing the existence is tantamount to disclosure of the restricted protected health information so as to not violate the agreed to restriction.

Comment: A few commenters said that covered entities should have the right to modify or revoke an agreement to restrict use or disclosure of protected health information.

Response: We agree that, as circumstances change, covered entities should be able to revisit restrictions to which they had previously agreed. At the same time, individuals should be able to rely on agreements to restrict the use or disclosure of information that they believe is particularly sensitive. If a covered entity would like to revoke or modify an agreed-upon restriction, the covered entity must renegotiate the agreement with the individual. If the individual agrees to modify or terminate the restriction, the covered entity must get written agreement from the individual or must document the oral agreement. If the individual does not agree to terminate or modify the restriction, the covered entity must inform the individual that it is modifying or terminating its agreement to the restriction and any modification or termination would apply only with respect to protected health information created or received after the covered entity informed the individual of the termination. Any protected health information created or received during the time between when the restriction was agreed to and when the covered entity informed the individual or such modification or termination remains subject to the restriction.

Comment: Many commenters advocated for stronger rights to request restrictions, particularly that victims of domestic violence should have an absolute right to restrict disclosure of information.

Response: We address restrictions for disclosures in two different ways, the right to request restrictions (§ 164.522(a)) and confidential communications (§ 164.522(b)). We have provided all individuals with a right to request restrictions on uses or disclosures of treatment, payment, and health care operations. This is not an absolute right to restrict. Covered entities are not required to agree to requested restrictions; however, if they do, the rule would require them to act in accordance with the restrictions. (See the preamble regarding § 164.522 for a more comprehensive discussion of the right to request restrictions.)

In the final rule, we create a new provision that provides individuals with a right to confidential communications, in response to these comments. This provision grants individuals with a right to restrict disclosures of information related to communications made by a covered entity to the individual, by allowing the individual to request that such communications be made to the person at an alternative location or by an alternative means. For example, a woman who lives with an abusive man and is concerned that his knowledge of her health care treatment may lead to additional abuse can request that any mail from the provider be sent to a friend's home or that telephone calls by a covered provider be made to her at work. Other reasonable accommodations may be requested as well, such as requesting that a covered provider never contact the individual by a phone, but only contact her by electronic mail. A provider must accommodate an individual's request for confidential communications, under this section, without requiring an explanation as to the reason for the request as a condition of accommodating the request. The individual does not need to be in an abusive situation to make such requests of a covered provider. The only conditions that a covered provider may place on an individual is that the request be reasonable with respect to the administrative burden on the provider, the request to be in writing, the request specify an alternative address or other method of contact, and that (where relevant) the individual provide information about how payment will be handled. What is reasonable may vary by the size or type of covered entity; however, additional modest cost to the provider would not be unreasonable.

An individual also has a right to restrict communications from a health plan. The right is the same as with covered providers except it is limited to cases where the disclosure of information could endanger the individual. A health plan may require an individual to state this fact as a condition of accommodating the individual's request for confidential communications. This would provide victims of domestic violence the right to control such disclosures.

Comment: Commenters opposed the provision of the NPRM (§ 164.506(c)(1)(ii)(B)) stating that an individual's right to request restrictions on use or disclosure of protected health information would not apply in emergency situations as set forth in proposed § 164.510(k). Commenters asserted that victims who have been harmed by violence may first turn to emergency services for help and that, in such situations, the victim should be able to request that the perpetrator not be told of his or her condition or whereabouts.

Response: We agree with some of the commenters' concerns. In the final rule, the right to request restrictions is available to all individuals regardless of the circumstance or the setting in which the individual is obtaining care. For example, an individual that seeks care in an emergency room has the same right to request a restriction as an individual seeking care in the office of a covered physician.

However, we continue to permit a covered entity to disclose protected health information to a health care

provider in an emergency treatment situation if the restricted protected health information is needed to provide the emergency treatment or if the disclosure is necessary to avoid serious and imminent threats to public health and safety. Although we understand the concern of the commenters, we believe that these exceptions are limited and will not cause a covered entity to disclose information to a perpetrator of a crime. We are concerned that a covered provider would be required to delay necessary care if a covered entity had to determine if a restriction exists at the time of such emergency. Even if a covered entity knew that there was a restriction, we permitted this limited exception for emergency situations because, as we had stated in the preamble for § 164.506 of the NPRM, an emergency situation may not provide sufficient opportunity for a patient and health care provider to discuss the potential implications of restricting use and disclosure of protected health information on that emergency. We also believe that the importance of avoiding serious and imminent threats to health and safety and the ethical and legal obligations of covered health care providers' to make disclosures for these purposes is so significant that it is not appropriate to apply the right to request restrictions on such disclosures.

We note that we have included other provisions in the final rule intended to avoid or minimize harm to victims of domestic violence. Specifically, we include provisions in the final rule that allow individuals to opt out of certain types of disclosures and require covered entities to use professional judgment to determine whether disclosure of protected health information is in a patient's best interest (see § 164.510(a) on use and disclosure for facility directories and § 164.510(b) on uses and disclosures for assisting in an individual's care and notification purposes). Although an agreed to restriction under § 164.522 would apply to uses and disclosures for assisting in an individual's care, the opt out provision in § 164.510(b) can be more helpful to a person who is a victim of domestic violence because the individual can opt out of such disclosure without obtaining the agreement of the covered provider. We permit a covered entity to elect not to treat a person as a personal representative (see § 164.502(g)) or to deny access to a personal representative (see § 164.524(a)(3)(iii)) where there are concerns related to abuse. We also include a new § 164.512(c) which recognizes the unique circumstances surrounding disclosure of protected health information about victims of abuse, neglect, and domestic violence.

Section 164.522(b)—Confidential Communications Requirements

Comment: Several commenters requested that we add a new section to prevent disclosure of sensitive health care services to members of the patient's family through communications to the individual's home, such as appointment notices, confirmation or scheduling of appointments, or mailing a bill or explanation of benefits, by requiring covered entities to agree to correspond with the patient in another way. Some commenters stated that this is necessary in order to protect inadvertent disclosure of sensitive information and to protect victims of domestic violence from disclosure to an abuser. A few commenters suggested that a covered entity should be required to obtain an individual's authorization prior to communicating with the individual at the individual's home with respect to health care relating to sensitive subjects such as reproductive health, sexually transmissible diseases, substance abuse or mental health.

Response: We agree with commenters' concerns regarding covered entities' communications with individuals. We created a new provision, § 164.522(b), to address confidential communications by covered entities. This provision gives individuals the right to request that they receive communications from covered entities at an alternative address or by an alternative means, regardless of the nature of the protected health information involved. Covered providers are required to accommodate reasonable requests by individuals and may not require the individual to explain the basis for the request as a condition of accommodation. Health plans are required to accommodate reasonable requests by individuals as well; however, they may require the individual to provide a statement that disclosure of the information could endanger the individual, and they may condition the accommodation on the receipt of such statement.

Under the rule, we have required covered providers to accommodate requests for communications to alternative addresses or by alternative means, regardless of the reason, to limit risk of harm. Providers have more frequent one-on-one communications with patients, making the safety concerns from an inadvertent disclosure more substantial and the need for confidential communications more compelling. We have made the requirement for covered providers absolute and not contingent on the reason for the request because we wanted to make it relatively easy for victims of domestic violence, who face real safety concerns by disclosures of health information, to limit the potential for such disclosures.

The standard we created for health plans is different from the requirement for covered providers, in that we only require health plans to make requested accommodations for confidential communications when the individual asserts that disclosure could be dangerous to the individual. We address health plan requirements in this way because health plans are often issued to a family member (the employee), rather than to each individual member of a family, and therefore, health plans tend to communicate with the named insured rather than with individual family members. Requiring plans to accommodate a restriction for one individual could be administratively more difficult than it is for providers that regularly communicate with individuals. However, in the case of domestic violence or potential abuse, the level of harm that can result from a disclosure of protected health information tips the balance in favor of requiring such restriction to prevent inadvertent disclosure. We have adopted the policy recommended by the National Association of Insurance Commissioners in the Health Information Policy Model Act (1998) as this best reflects the balance of the appropriate level of regulation of the industry compared with the need to protect individuals from harm that may result from inadvertent disclosure of information. This policy is also consistent with recommendations made in the Family Violence Prevention Fund's publication ''Health Privacy Principles for Protecting Victims of Domestic Violence'' (October 2000). Of course, health plans may accommodate requests for confidential communications without requiring a statement that the individual would be in danger from disclosure of protected health information.

Comment: One commenter requested that we create a standard that all information from a health plan be sent to the patient and not the policyholder or subscriber.

Response: We require health plans to accommodate certain requests that information not be sent to a particular location or by particular means. A health plan must accommodate reasonable requests by individuals that protected health information about them be sent directly to them and not to a policyholder or subscriber, if the

individual states that he or she may be in danger from disclosure of such information. We did not generally require health plans to send information to the patient and not the policyholder or subscriber because we believed it would be administratively burdensome and because the named insured may have a valid need for such information to manage payment and benefits.

Sensitive Subjects

Comment: Many commenters requested that additional protections be placed on sensitive information, including information regarding HIV/AIDS, sexually transmitted diseases, mental health, substance abuse, reproductive health, and genetics. Many requested that we ensure the regulation adequately protects victims of domestic violence. They asserted that the concern for discrimination or stigma resulting from disclosure of sensitive health information could dissuade a person from seeking needed treatment. Some commenters noted that many state laws provide additional protections for various types of information. They requested that we develop federal standards to have consistent rules regarding the protection of sensitive information to achieve the goals of cost savings and patient protection. Others requested that we require patient consent or special authorization before certain types of sensitive information was disclosed, even for treatment, payment, and health care operations, and some thought we should require a separate request for each disclosure. Some commenters requested that the right to request restrictions be replaced with a requirement for an authorization for specific types of sensitive information. There were recommendations that we require covered entities to develop internal policies to address sensitive information.

Other commenters argued that sensitive information should not be segregated from the record because it may limit a future provider's access to information necessary for treatment of the individual and it could further stigmatize a patient by labeling him or her as someone with sensitive health care issues. These commenters further maintained that segregation of particular types of information could negatively affect analysis of community needs, research, and would lead to higher costs of health care delivery.

Response: We generally do not differentiate among types of protected health information, because all health information is sensitive. The level of sensitivity varies not only with the type of information, but also with the individual and the particular situation faced by the individual. This is demonstrated by the different types of information that commenters singled out as meriting special protection, and in the great variation among state laws in defining and protecting sensitive information. Most states have a law providing heightened protection for some type of health information. However, even though most states have considered the issue of sensitive information, the variation among states in the type of information that is specially protected and the requirements for permissible disclosure of such information demonstrates that there is no national consensus.

Where, as in this case, most states have acted and there is no predominant rule that emerges from the state experience with this issue, we have decided to let state law predominate. The final rule only provides a floor of protection for health information and does not preempt state laws that provide greater protection than the rule. Where states have decided to treat certain information as more sensitive than other information, we do not preempt those laws.

To address the variation in the sensitivity of protected health information without defining specially sensitive information, we incorporate opportunities for individuals and covered entities to address specific sensitivities and concerns about uses and disclosures of certain protected health information that the patient and provider believe are particularly sensitive, as follows:

- Covered entities are required to provide individuals with notice of their privacy practices and give individuals the opportunity to request restrictions of the use and disclosure of protected health information by the covered entity. (See § 164.522(a) regarding right to request restrictions.)
- Individuals have the right to request, and in some cases require, that communications from the covered entity to them be made to an alternative address or by an alternative means than the covered entity would otherwise use. (See § 164.522(b) regarding confidential communications.)
- Covered entities have the opportunity to decide not to treat a person as a personal representative when the covered entity has a reasonable belief that an individual has been subjected to domestic violence, abuse, or neglect by such person or that treating such person as a personal representative could endanger the individual. (See § 164.502(g)(5) regarding personal representatives.)
- Covered entities may deny access to protected health information when there are concerns that the access may result in varying levels of harm. (See § 164.524(a)(3) regarding denial of access.)
- Covered health care providers may, in some circumstances and consistent with any known prior preferences of the individual, exercise professional judgment in the individual's best interest to not disclose directory information. (See § 164.510(a) regarding directory information.)
- Covered entities may, in some circumstances, exercise professional judgment in the individual's best interest to limit disclosure to persons assisting in the individual's care. (See § 164.510(b) regarding persons assisting in the individual's care.)

This approach allows for state law and personal variation in this area.

The only type of protected health information that we treat with heightened protection is psychotherapy notes. We provide a different level of protection because they are unique types of protected health information that typically are not used or required for treatment, payment, or health care operations other than by the mental health professional that created the notes. (See § 164.508(a)(2) regarding psychotherapy notes.)

Section 164.524—Access of Individuals to Protected Health Information

Comment: Some commenters recommended that there be no access to disease registries.

Response: Most entities that maintain disease registries are not covered entities under this regulation; examples of such non-covered entities are public health agencies and pharmaceutical companies. If, however, a disease registry is maintained by a covered entity and is used to make decisions about individuals, this rule requires the covered entity to provide access to information about a requesting individual unless one of the rule's conditions for denial of access is met. We found no persuasive reasons why disease registries should be given special treatment compared with other information that may be used to make decisions about an individual.

Comment: Some commenters stated that covered entities should be held accountable for access to information held by business partners so that individuals would not have the burden of tracking down their protected health information from a business partner. Many commenters, including insurers

and academic medical centers, recommended that, to reduce burden and duplication, only the provider who created the protected health information should be required to provide individuals access to the information. Commenters also asked that other entities, including business associates, the Medicare program, and pharmacy benefit managers, not be required to provide access, in part because they do not know what information the covered entity already has and they may not have all the information requested. A few commenters also argued that billing companies should not have to provide access because they have a fiduciary responsibility to their physician clients to maintain the confidentiality of records.

Response: A general principle in responding to all of these points is that a covered entity is required to provide access to protected health information in accordance with the rule regardless of whether the covered entity created such information or not. Thus, we agree with the first point: in order to meet its requirements for providing access, a covered entity must not only provide access to such protected health information it holds, but must also provide access to such information in a designated record set of its business associate, pursuant to its business associate contract, unless the information is the same as information maintained directly by the covered entity. We require this because an individual may not be aware of business associate relationships. Requiring an individual to track down protected health information held by a business associate would significantly limit access. In addition, we do not permit a covered entity to limit its duty to provide access by giving protected health information to a business associate.

We disagree with the second point: if the individual directs an access request to a covered entity that has the protected health information requested, the covered entity must provide access (unless it may deny access in accordance with this rule). In order to assure that an individual can exercise his or her access rights, we do not require the individual to make a separate request to each originating provider. The originating provider may no longer be in business or may no longer have the information, or the non-originating provider may have the information in a modified or enhanced form.

We disagree with the third point: other entities must provide access only if they are covered entities or business associates of covered entities, and they must provide access only to protected health information that they maintain (or that their business associates maintain). It would not be efficient to require a covered entity to compare another entity's information with that of the entity to which the request was addressed. (See the discussion regarding covered entities for information about whether a pharmacy benefit manager is a covered entity.)

We disagree with the fourth point: a billing company will be required by its business associate contract only to provide the requested protected health information to its physician client. This action will not violate any fiduciary responsibility. The physician client would in turn be required by the rule to provide access to the individual.

Comment: Some commenters asked for clarification that the clearinghouse function of turning non-standardized data into standardized data does not create non-duplicative data and that ''duplicate'' does not mean ''identical.'' A few commenters suggested that duplicated information in a covered entity's designated record set be supplied only once per request.

Response: We consider as duplicative information the same information in different formats, media, or presentations, or which have been standardized. Business associates who have materially altered protected health information are obligated to provide individuals access to it. Summary information and reports, including those of lab results, are not the same as the underlying information on which the summaries or reports were based. A clean document is not a duplicate of the same document with notations. If the same information is kept in more than one location, the covered entity has to produce the information only once per request for access.

Comment: A few commenters suggested requiring covered entities to disclose to third parties without exception at the requests of individuals. It was argued that this would facilitate disability determinations when third parties need information to evaluate individuals' entitlement to benefits. Commenters argued that since covered entities may deny access to individuals under certain circumstances, individuals must have another method of providing third parties with their protected health information.

Response: We allow covered entities to forward protected health information about an individual to a third party, pursuant to the individual's authorization under § 164.508. We do not require covered entities to disclose information pursuant to such authorizations because the focus of the rule is privacy of protected health information. Requiring disclosures in all circumstances would be counter to this goal. In addition, a requirement of disclosing protected health information to a third party is not a necessary substitute for the right of access to individuals, because we allow denial of access to individuals under rare circumstances. However, if the third party is a personal representative of the individual in accordance with § 164.502(g) and there is no concern regarding abuse or harm to the individual or another person, we require the covered entity to provide access to that third party on the individual's behalf, subject to specific limitations. We note that a personal representative may obtain access on the individual's behalf in some cases where covered entity may deny access to the individual. For example, an inmate may be denied a copy of protected health information, but a personal representative may be able to obtain a copy on the individual's behalf. See § 164.502(g) and the corresponding preamble discussion regarding the ability of a personal representative to act on an individual's behalf.

Comment: The majority of commenters supported granting individuals the right to access protected health information for as long as the covered entity maintains the protected health information; commenters argued that to do otherwise would interfere with existing record retention laws. Some commenters advocated for limiting the right to information that is less than one or two years old. A few commenters explained that frequent changes in technology makes it more difficult to access stored data. The commenters noted that the information obtained prior to the effective date of the rule should not be required to be accessible.

Response: We agree with the majority of commenters and retain the proposal to require covered entities to provide access for as long as the entity maintains the protected health information. We do not agree that information created prior to the effective date of the rule should not be accessible. The reasons for granting individuals access to information about them do not vary with the date the information was created.

Comment: A few commenters argued that there should be no grounds for denying access, stating that individuals should always have the right to inspect and copy their protected health information.

Response: While we agree that in the vast majority of instances individuals should have access to information about them, we cannot agree that a blanket rule would be appropriate. For example, where a professional familiar with the particular circumstances believes that providing such access is likely to endanger a person's life or physical safety, or where granting such access would violate the privacy of other individuals, the benefits of allowing access may not outweigh the harm. Similarly, we allow denial of access where disclosure would reveal the source of confidential information because we do not want to interfere with a covered entity's ability to maintain implicit or explicit promises of confidence.

We create narrow exceptions to the rule of open access, and we expect covered entities to employ these exceptions rarely, if at all. Moreover, we require covered entities to provide access to any protected health information requested after excluding only the information that is subject to a denial. The categories of permissible denials are not mandatory, but are a means of preserving the flexibility and judgment of covered entities under appropriate circumstances.

Comment: Many commenters supported our proposal to allow covered entities to deny an individual access to protected health information if a professional determines either that such access is likely to endanger the life or physical safety of a person or, if the information is about another person, access is reasonably likely to cause substantial harm to such person.

Some commenters requested that the rule also permit covered entities to deny a request if access might be reasonably likely to cause psychological or mental harm, or emotional distress. Other commenters, however, were particularly concerned about access to mental health information, stating that the lack of access creates resentment and distrust in patients.

Response: We disagree with the comments suggesting that we expand the grounds for denial of access to an individual to include a likelihood of psychological or mental harm of the individual. We did not find persuasive evidence that this is a problem sufficient to outweigh the reasons for providing open access. We do allow a denial for access based on a likelihood of substantial psychological or mental harm, but only if the protected health information includes information about another person and the harm may be inflicted on such other person or if the person requesting the access is a personal representative of the individual and the harm may be inflicted on the individual or another person.

We generally agree with the commenters concerns that denying access specifically to mental health records could create distrust. To balance this concern with other commenters' concerns about the potential for psychological harm, however, we exclude psychotherapy notes from the right of access. This is the only distinction we make between mental health information and other types of protected health information in the access provisions of this rule. Unlike other types of protected health information, these notes are not widely disseminated through the health care system. We believe that the individual's privacy interests in having access to these notes, therefore, are outweighed by the potential harm caused by such access. We encourage covered entities that maintain psychotherapy notes, however, to provide individuals access to these notes when they believe it is appropriate to do so.

Comment: Some commenters believed that there is a potential for abuse of the provision allowing denial of access because of likely harm to self. They questioned whether there is any experience from the Privacy Act of 1974 to suggest that patients who requested and received their records have ever endangered themselves as a result.

Response: We are unaware of such problems from access to records that have been provided under the Privacy Act but, since these are private matters, such problems might not come to our attention. We believe it is more prudent to preserve the flexibility and judgment of health care professionals familiar with the individuals and facts surrounding a request for records than to impose the blanket rule suggested by these commenters.

Comment: Commenters asserted that the NPRM did not adequately protect vulnerable individuals who depend on others to exercise their rights under the rule. They requested that the rule permit a covered entity to deny access when the information is requested by someone other than the subject of the information and, in the opinion of a licensed health care professional, access to the information could harm the individual or another person.

Response: We agree with the commenters that such protection is warranted and add a provision in § 164.524(a)(3), which permits a covered health care provider to deny access if a personal representative of the individual is making the request for access and a licensed health care professional has determined, in the exercise of professional judgment, that providing access to such personal representative could result in substantial harm to the individual or another person. Access can be denied even if the potential harm may be inflicted by someone other than the personal representative.

This provision is designed to strike a balance between the competing interests of ensuring access to protected health information and protecting the individual or others from harm. The ''substantial harm'' standard will ensure that a covered entity cannot deny access in cases where the harm is de minimus.

The amount of discretion that a covered entity has to deny access to a personal representative is generally greater than the amount of discretion that a covered entity has to deny access to an individual. Under the final rule, a covered entity may deny access to an individual if a licensed health care professional determines that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. In this case, concerns about psychological or emotional harm would not be sufficient to justify denial of access. We establish a relatively high threshold because we want to assure that individuals have broad access to health information about them, and due to the potential harm that comes from denial of access, we believe denials should be permitted only in limited circumstances.

The final rule grants covered entities greater discretion to deny access to a personal representative than to an individual in order to provide protection to those vulnerable people who depend on others to exercise their rights under the rule and who may be subjected to abuse or neglect. This provision applies to personal representatives of minors as well as other individuals. The same standard for denial of access on the basis of potential harm that applies to personal representatives also applies when an individual is seeking access to his or her protected health information, and the information makes reference to another person. Under these circumstances, a covered entity may deny a request for access if such access is reasonably likely to cause substantial harm to such other person. The standard for this provision and for the provision regarding access by personal representatives is the same because both circumstances involve one person obtaining information about another person, and in both cases the covered entity is balancing the right of access of one person against the right of

a second person not to be harmed by the disclosure.

Under any of these grounds for denial of access to protected health information, the covered entity is not required to deny access to a personal representative under these circumstances, but has the discretion to do so.

In addition to denial of access rights, we also address the concerns raised by abusive or potentially abusive situations in the section regarding personal representatives by giving covered entities discretion to not recognize a person as a personal representative of an individual if the covered entity has a reasonable belief that the individual has been subjected to domestic violence, abuse, or neglect by or would be in danger from a person seeking to act as the personal representative. (See § 164.502(g))

Comment: A number of commenters were concerned that this provision would lead to liability for covered entities if the release of information results in harm to individuals. Commenters requested a ''good faith'' standard in this provision to relieve covered entities of liability if individuals suffer harm as a result of seeing their protected health information or if the information is found to be erroneous. A few commenters suggested requiring providers (when applicable) to include with any disclosure to a third party a statement that, in the provider's opinion, the information should not be disclosed to the patient.

Response: We do not intend to create a new duty to withhold information nor to affect other laws on this issue. Some state laws include policies similar to this rule, and we are not aware of liability arising as a result.

Comment: Some commenters suggested that both the individual's health care professional and a second professional in the relevant field of medicine should review each request. Many commenters suggested that individuals have a right to have an independent review of any denial of access, e.g., review by a health care professional of the individual's choice.

Response: We agree with the commenters who suggest that denial on grounds of harm to self or others should be determined by a health professional, and retain this requirement in the final rule. We disagree, however, that all denials should be reviewed by a professional of the individual's choice. We are concerned that the burden such a requirement would place on covered entities would be significantly greater than any benefits to the individual. We believe that any health professional, not just one of the individual's choice, will exercise appropriate professional judgment. To address some of these concerns, however, we add a provision for the review of denials requiring the exercise of professional judgment. If a covered entity denies access based on harm to self or others, the individual has the right to have the denial reviewed by another health care professional who did not participate in the original decision to deny access.

Comment: A few commenters objected to the proposal to allow covered entities to deny a request for access to health information if the information was obtained from a confidential source that may be revealed upon the individual's access. They argued that this could be subject to abuse and the information could be inherently less reliable, making the patient's access to it even more important.

Response: While we acknowledge that information provided by confidential sources could be inaccurate, we are concerned that allowing unfettered access to such information could undermine the trust between a health care provider and patients other than the individual. We retain the proposed policy because we do not want to interfere with a covered entity's ability to obtain important information that can assist in the provision of health care or to maintain implicit or explicit promises of confidence, which may be necessary to obtain such information. We believe the concerns raised about abuse are mitigated by the fact that the provision does not apply to promises of confidentiality made to a health care provider. We note that a covered entity may provide access to such information.

Comment: Some commenters were concerned that the NPRM did not allow access to information unrelated to treatment, and thus did not permit access to research information.

Response: In the final rule, we eliminate the proposed special provision for ''research information unrelated to treatment.'' The only restriction on access to research information in this rule applies where the individual agrees in advance to denial of access when consenting to participate in research that includes treatment. In this circumstance, the individual's right of access to protected health information created in the course of the research may be suspended for as long as the research is in progress, but access rights resume after such time. In other instances, we make no distinction between research information and other information in the access provisions in this rule.

Comment: A few commenters supported the proposed provision temporarily denying access to information obtained during a clinical trial if participants agreed to the denial of access when consenting to participate in the trial. Some commenters believed there should be no access to any research information. Other commenters believed denial should occur only if the trial would be compromised. Several recommended conditioning the provision. Some recommended that access expires upon completion of the trial unless there is a health risk. A few commenters suggested that access should be allowed only if it is included in the informed consent and that the informed consent should note that some information may not be released to the individual, particularly research information that has not yet been validated. Other commenters believed that there should be access if the research is not subject to IRB or privacy board review or if the information can be disclosed to third parties.

Response: We agree with the commenters that support temporary denial of access to information from research that includes treatment if the subject has agreed in advance, and with those who suggested that the denial of access expire upon completion of the research, and retain these provisions in the final rule. We disagree with the commenters who advocate for further denial of this information. These comments did not explain why an individual's interest in access to health information used to make decisions about them is less compelling with respect to research information. Under this rule, all protected health information for research is subject either to privacy board or IRB review unless a specific authorization to use protected health information for research is obtained from the individual. Thus, this is not a criterion we can use to determine access rights.

Comment: A few commenters believed that it would be ''extremely disruptive of and dangerous'' to patients to have access to records regarding their current care and that state law provides sufficient protection of patients' rights in this regard.

Response: We do not agree. Information about current care has immediate and direct impact on individuals. Where a health care professional familiar with the circumstances believes that it is reasonably likely that access to records would endanger the life or physical safety of the individual or another

person, the regulation allows the professional to withhold access.

Comment: Several commenters requested clarification that a patient not be denied access to protected health information because of failure to pay a bill. A few commenters requested clarification that entities may not deny requests simply because producing the information would be too burdensome.

Response: We agree with these comments, and confirm that neither failure to pay a bill nor burden are lawful reasons to deny access under this rule. Covered entities may deny access only for the reasons provided in the rule.

Comment: Some commenters requested that the final rule not include detailed procedural requirements about how to respond to requests for access. Others made specific recommendations on the procedures for providing access, including requiring written requests, requiring specific requests instead of blanket requests, and limiting the frequency of requests. Commenters generally argued against requiring covered entities to acknowledge requests, except under certain circumstances, because of the potential burden on entities.

Response: We intend to provide sufficient procedural guidelines to ensure that individuals have access to their protected health information, while maintaining the flexibility for covered entities to implement policies and procedures that are appropriate to their needs and capabilities. We believe that a limit on the frequency of requests individuals may make would arbitrarily infringe on the individual's right of access and have, therefore, not included such a limitation. To limit covered entities' burden, we do not require covered entities to acknowledge receipt of the individuals' requests, other than to notify the individual once a decision on the request has been made. We also permit a covered entity to require an individual to make a request for access in writing and to discuss a request with an individual to clarify which information the individual is actually requesting. If individuals agree, covered entities may provide access to a subset of information rather than all protected health information in a designated record set. We believe these changes provide covered entities with greater flexibility without compromising individuals' access rights.

Comment: Commenters offered varying suggestions for required response time, ranging from 48 hours because of the convenience of electronic records to 60 days because of the potential burden. Others argued against a finite time period, suggesting the response time be based on mutual convenience of covered entities and individuals, reasonableness, and exigencies. Commenters also varied on suggested extension periods, from one 30-day extension to three 30-day extensions to one 90-day extension, with special provisions for off-site records.

Response: We are imposing a time limit because individuals are entitled to know when to expect a response. Timely access to protected health information is important because such information may be necessary for the individual to obtain additional health care services, insurance coverage, or disability benefits, and the covered entity may be the only source for such information. To provide additional flexibility, we eliminate the requirement that access be provided as soon as possible and we lengthen the deadline for access to off-site records. For on-site records, covered entities must act on a request within 30 days of receipt of the request. For off-site records, entities must complete action within 60 days. We also permit covered entities to extend the deadline by up to 30 days if they are unable to complete action on the request within the standard deadline. These time limits are intended to be an outside deadline rather than an expectation. We expect covered entities to be attentive to the circumstances surrounding each request and respond in an appropriate time frame.

Comment: A few commenters suggested that, upon individuals' requests, covered entities should be required to provide protected health information in a format that would be understandable to a patient, including explanations of codes or abbreviations. The commenters suggested that covered entities be permitted to provide summaries of pertinent information instead of full copies of records; for example, a summary may be more helpful for the patient's purpose than a series of indecipherable billing codes.

Response: We agree with these commenters' point that some health information is difficult to interpret. We clarify, therefore, that the covered entity may provide summary information in lieu of the underlying records. A summary may only be provided if the covered entity and the individual agree, in advance, to the summary and to any fees imposed by the covered entity for providing such summary. We similarly permit a covered entity to provide an explanation of the information. If the covered entity charges a fee for providing an explanation, it must obtain the individual's agreement to the fee in advance.

Comment: Though there were recommendations that fees be limited to the costs of copying, the majority of commenters on this topic requested that covered entities be able to charge a reasonable, cost-based fee. Commenters suggested that calculation of access costs involve factors such as labor costs for verification of requests, labor and software costs for logging of requests, labor costs for retrieval, labor costs for copying, expense costs for copying, capital cost for copying, expense costs for mailing, postal costs for mailing, billing and bad-debt expenses, and labor costs for refiling. Several commenters recommended specific fee structures.

Response: We agree that covered entities should be able to recoup their reasonable costs for copying of protected health information, and include such provision in the regulation. We are not specifying a set fee because copying costs could vary significantly depending on the size of the covered entity and the form of such copy (*e.g.,* paper, electronic, film). Rather, covered entities are permitted to charge a reasonable, cost-based fee for copying (including the costs of supplies and labor), postage, and summary or explanation (if requested and agreed to by the individual) of information supplied. The rule limits the types of costs that may be imposed for providing access to protected health information, but does not preempt applicable state laws regarding specific allowable fees for such costs. The inclusion of a copying fee is not intended to impede the ability of individuals to copy their records.

Comment: Many commenters stated that if a covered entity denies a request for access because the entity does not hold the protected health information requested, the covered entity should provide, if known, the name and address of the entity that holds the information. Some of these commenters additionally noted that the Uniform Insurance Information and Patient Protection Act, adopted by 16 states, already imposes this notification requirement on insurance entities. Some commenters also suggested requiring providers who leave practice or move offices to inform individuals of that fact and of how to obtain their records.

Response: We agree that, when covered entities deny requests for access because they do not hold the protected health information requested, they should inform individuals of the holder of the information, if known; we include this provision in the final rule. We do not require health care providers to

notify all patients when they move or leave practice, because the volume of such notifications would be unduly burdensome.

Section 164.526—Amendment of Protected Health Information

Comment: Many commenters strongly encouraged the Secretary to adopt ''appendment'' rather than ''amendment and correction'' procedures. They argued that the term ''correction'' implies a deletion of information and that the proposed rule would have allowed covered entities to remove portions of the record at their discretion. Commenters indicated that appendment rather than correction procedures will ensure the integrity of the medical record and allow subsequent health care providers access to the original information as well as the appended information. They also indicated appendment procedures will protect both individuals and covered entities since medical records are sometimes needed for litigation or other legal proceedings.

Response: We agree with commenters' concerns about the term ''correction.'' We have revised the rule and deleted ''correction'' from this provision in order to clarify that covered entities are not required by this rule to delete any information from the designated record set. We do not intend to alter medical record retention laws or current practice, except to require covered entities to append information as requested to ensure that a record is accurate and complete. If a covered entity prefers to comply with this provision by deleting the erroneous information, and applicable record retention laws allow such deletion, the entity may do so. For example, an individual may inform the entity that someone else's X-rays are in the individual's medical record. If the entity agrees that the X-ray is inaccurately filed, the entity may choose to so indicate and note where in the record the correct X-ray can be found. Alternatively, the entity may choose to remove the X-ray from the record and replace it with the correct X-ray, if applicable law allows the entity to do so. We intend the term ''amendment'' to encompass either action.

We believe this approach is consistent with well-established privacy principles, with other law, and with industry standards and ethical guidelines. The July 1977 Report of the Privacy Protection Study Commission recommended that health care providers and other organizations that maintain medical-record information have procedures for individuals to correct or amend the information.[28] The Privacy Act (5 U.S.C. 552a) requires government agencies to permit individuals to request amendment of any record the individual believes is not accurate, relevant, timely, or complete. In its report ''Best Principles for Health Privacy,'' the Health Privacy Working Group recommended, ''An individual should have the right to supplement his or her own medical record. Supplementation should not be implied to mean deletion or alteration of the medical record.'' [29] The National Association of Insurance Commissioners' Health Information Privacy Model Act establishes the right of an individual who is the subject of protected health information to amend protected health information to correct any inaccuracies. The National Conference of Commissioners on Uniform State Laws' Uniform Health Care Information Act states, ''Because accurate health-care information is not only important to the delivery of health care, but for patient applications for life, disability and health insurance, employment, and a great many other issues that might be involved in civil litigation, this Act allows a patient to request an amendment in his record.''

Some states also establish a right for individuals to amend health information about them. For example, Hawaii law (HRS section 323C–12) states, ''An individual or the individual's authorized representative may request in writing that a health care provider that generated certain health care information append additional information to the record in order to improve the accuracy or completeness of the information; provided that appending this information does not erase or obliterate any of the original information.'' Montana law (MCA section 50–16–543) states, ''For purposes of accuracy or completeness, a patient may request in writing that a health care provider correct or amend its record of the patient's health care information to which he has access.'' Connecticut, Georgia, and Maine provide individuals a right to request correction, amendment, or deletion of recorded personal information about them maintained by an insurance institution. Many other states have similar provisions.

Industry and standard-setting organizations have also developed policies for amendment of health information. The National Committee for Quality Assurance and the Joint Commission on Accreditation of Healthcare Organizations issued recommendations stating, ''The opportunity for patients to review their records will enable them to correct any errors and may provide them with a better understanding of their health status and treatment. Amending records does not erase the original information. It inserts the correct information with a notation about the date the correct information was available and any explanation about the reason for the error.'' [30] Standards of the American Society for Testing and Materials state, ''An individual has a right to amend by adding information to his or her record or database to correct inaccurate information in his or her patient record and in secondary records and databases which contain patient identifiable health information.'' [31] We build on this well-established principle in this final rule.

Comment: Some commenters supported the proposal to allow individuals to request amendment for as long as the covered provider or plan maintains the information. A few argued that the provision should be time-limited, *e.g.,* that covered entities should not have to amend protected health information that is more than two years old. Other comments suggested that the provision should only be applied to protected health information created after the compliance date of the regulation.

Response: The purpose of this provision is to create a mechanism whereby individuals can ensure that information about them is as accurate as possible as it travels through the health care system and is used to make decisions, including treatment decisions, about them. To achieve this result, individuals must have the ability to request amendment for as long as the information used to make decisions about them exists. We therefore retain the proposed approach. For these reasons, we also require covered entities to address requests for amendment of all protected health information within designated record sets, including information created or obtained prior to

[28] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 300–303.

[29] Health Privacy Working Group, ''Best Principles for Health Privacy,'' Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, July 1999.

[30] National Committee on Quality Assurance and the Joint Commission on Accreditation of Healthcare Organizations, ''Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment,''1998, p. 25.

[31] ASTM, ''Standard Guide for Confidentiality, Privacy, Access and Data Security, Principles for Health Information Including Computer-Based Patient Records,'' E 1869–97, § 11.1.1.

the compliance date, for as long as the entity maintains the information.

Comment: A few commenters were concerned that the proposal implied that the individual is in control of and may personally change the medical record. These commenters opposed such an approach.

Response: We do not give individuals the right to alter their medical records. Individuals may request amendment, but they have no authority to determine the final outcome of the request and may not make actual changes to the medical record. The covered entity must review the individual's request and make appropriate decisions. We have clarified this intent in § 164.526(a)(1) by stating that individuals have a right to have a covered entity amend protected health information and in § 164.526(b)(2) by stating that covered entities must act on an individual's request for amendment.

Comment: Some comments argued that there is no free-text field in some current transaction formats that would accommodate the extra text required to comply with the amendment provisions (*e.g.,* sending statements of disagreement along with all future disclosures of the information at issue). Commenters argued that this provision will burden the efficient transmission of information, contrary to HIPAA requirements.

Response: We believe that most amendments can be incorporated into the standard transactions as corrections of erroneous data. We agree that some of the standard transactions cannot currently accommodate additional material such as statements of disagreement and rebuttals to such statements. To accommodate these rare situations, we modify the requirements in § 164.526(d)(iii). The provision now states that if a standard transaction does not permit the inclusion of the additional material required by this section, the covered entity may separately transmit the additional material to the recipient of the standard transaction. Commenters interested in modifying the standard transactions to allow the incorporation of additional materials may also bring the issue up for resolution through the process established by the Transactions Rule and described in its preamble.

Comment: The NPRM proposed to allow amendment of protected health information in designated record sets. Some commenters supported the concept of a designated record set and stated that it appropriately limits the type of information available for amendment to information directly related to treatment. Other commenters were concerned about the burden this provision will create due to the volume of information that will be available for amendment. They were primarily concerned with the potential for frivolous, minor, or technical requests. They argued that for purposes of amendment, this definition should be limited to information used to make medical or treatment decisions about the individual. A few commenters requested clarification that individuals do not have a right to seek amendment unless there is verifiable information to support their claim or they can otherwise convince the entity that the information is inaccurate or incomplete.

Response: We believe that the same information available for inspection should also be subject to requests for amendment, because the purpose of these provisions is the same: To give consumers access to and the chance to correct errors in information that may be used to make decisions that affect their interests. We thus retain use of the ''designated record set'' in this provision. However, we share commenters'' concerns about the potential for minor or technical requests. To address this concern, we have clarified that covered entities may deny a request for amendment if the request is not in writing and does not articulate a reason to support the request, as long as the covered entity informs the individual of these requirements in advance.

Comment: Many commenters noted the potentially negative impact of the proposal to allow covered entities to deny a request for amendment if the covered entity did not create the information at issue. Some commenters pointed out that the originator of the information may no longer exist or the individual may not know who created the information in question. Other commenters supported the proposal that only the originator of the information is responsible for amendments to it. They argued that any extension of this provision requiring covered entities to amend information they have not created is administratively and financially burdensome.

Response: In light of the comments, we modify the rule to require the holder of the information to consider a request for amendment if the individual requesting amendment provides a reasonable basis to believe that the originator of the information is no longer available to act on a request. For example, if a request indicates that the information at issue was created by a hospital that has closed, and the request is not denied on other grounds, then the entity must amend the information. This provision is necessary to preserve an individual's right to amend protected health information about them in certain circumstances.

Comment: Some commenters stated that the written contract between a covered entity and its business associate should stipulate that the business associate is required to amend protected health information in accordance with the amendment provisions. Otherwise, these commenters argued, there would be a gap in the individual's right to have erroneous information corrected, because the covered entity could deny a request for amendment of information created by a business associate.

Response: We agree that information created by the covered entity or by the covered entity's business associates should be subject to amendment. This requirement is consistent with the requirement to make information created by a business associate available for inspection and copying. We have revised the rule to require covered entities to specify in the business associate contract that the business associate will make protected health information available for amendment and will incorporate amendments accordingly. (See § 164.504(e).)

Comment: One commenter argued that covered entities should be required to presume information must be corrected where an individual informs the entity that an adjudicative process has made a finding of medical identity theft.

Response: Identity theft is one of many reasons why protected health information may be inaccurate, and is one of many subjects that may result in an adjudicative process relevant to the accuracy of protective health information. We believe that this provision accommodates this situation without a special provision for identity theft.

Comment: Some commenters asserted that the proposed rule's requirement that action must be taken on individuals' requests within 60 days of the receipt of the request was unreasonable and burdensome. A few commenters proposed up to three 30-day extensions for ''extraordinary'' (as defined by the entity) requests.

Response: We agree that 60 days will not always be a sufficient amount of time to adequately respond to these requests. Therefore, we have revised this provision to allow covered entities the option of a 30-day extension to deal with requests that require additional response time. However, we expect that 60 days will be adequate for most cases.

Comment: One commenter questioned whether a covered entity could

appropriately respond to a request by amending the record, without indicating whether it believes the information at issue is accurate and complete.

Response: An amendment need not include a statement by the covered entity as to whether the information is or is not accurate and complete. A covered entity may choose to amend a record even if it believes the information at issue is accurate and complete. If a request for amendment is accepted, the covered entity must notify the individual that the record has been amended. This notification need not include any explanation as to why the request was accepted. A notification of a denied request, however, must contain the basis for the denial.

Comment: A few commenters suggested that when an amendment is made, the date should be noted. Some also suggested that the physician should sign the notation.

Response: We believe such a requirement would create a burden that is not necessary to protect individuals' interests, and so have not accepted this suggestion. We believe that the requirements of § 164.526(c) regarding actions a covered entity must take when accepting a request will provide an adequate record of the amendment. A covered entity may date and sign an amendment at its discretion.

Comment: The NPRM proposed that covered entities, upon accepting a request for amendment, make reasonable efforts to notify those persons the individual identifies, and other persons whom 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. Many commenters argued that this notification requirement was too burdensome and should be narrowed. They expressed concern that covered entities would have to notify anyone who might have received the information, even persons identified by the individual with whom the covered entity had no contact. Other commenters also contended that this provision would require covered entities to determine the reliance another entity might place on the information and suggested that particular part of the notification requirements be removed. Another commenter suggested that the notification provision be eliminated entirely, believing that it was unnecessary.

Response: Although there is some associated administrative burden with this provision, we believe it is a necessary requirement to effectively communicate amendments of erroneous or incomplete information to other parties. The negative effects of erroneous or incomplete medical information can be devastating. This requirement allows individuals to exercise some control in determining recipients they consider important to be notified, and requires the covered entity to communicate amendments to other persons that the covered entity knows have the erroneous or incomplete information and may take some action in reliance on the erroneous or incomplete information to the detriment of the individual. We have added language to clarify that the covered entity must obtain the individual's agreement to have the amendment shared with the persons the individual and covered entity identifies. We believe these notification requirements appropriately balance covered entities' burden and individuals' interest in protecting the accuracy of medical information used to make decisions about them. We therefore retain the notification provisions substantially as proposed.

Comment: Some commenters argued against the proposed provision requiring a covered entity that receives a notice of amendment to notify its business associates, ''as appropriate,'' of necessary amendments. Some argued that covered entities should only be required to inform business associates of these changes if the amendment could affect the individual's further treatment, citing the administrative and financial burden of notifying all business associates of changes that may not have a detrimental effect on the patient. Other commenters suggested that covered entities should only be required to inform business associates whom they reasonably know to be in possession of the information.

Response: We agree with commenters that clarification is warranted. Our intent is that covered entities must meet the requirements of this rule with respect to protected health information they maintain, including protected health information maintained on their behalf by their business associates. We clarify this intent by revising the definition of designated record set (see § 164.501) to include records maintained ''by or for'' a covered entity. Section 164.526(e) requires a covered entity that is informed of an amendment made by another covered entity to incorporate that amendment into designated record sets, whether the designated record set is maintained by the covered entity or for the covered entity by a business associate. If a business associate maintains the record at issue on the covered entity's behalf, the covered entity must fulfill its requirement by informing the business associate of the amendment to the record. The contract with the business associate must require the business associate to incorporate any such amendments. (See § 164.504(e).)

Comment: Some commenters supported the proposal to require covered entities to provide notification of the covered entity's statement of denial and the individual's statement of disagreement in any subsequent disclosures of the information to which the dispute relates. They argued that we should extend this provision to prior recipients of disputed information who have relied on it. These commenters noted an inconsistency in the proposed approach, since notification of accepted amendments is provided to certain previous recipients of erroneous health information and to recipients of future disclosures. They contended there is not a good justification for the different treatment and believed that the notification standard should be the same, regardless of whether the covered entity accepts the request for amendment.

These commenters also recommended that the individual be notified of the covered entity's intention to rebut a statement of disagreement. They suggested requiring covered entities to send a copy of the statement of rebuttal to the individual.

Response: Where a request for amendment is accepted, the covered entity knows that protected health information about the individual is inaccurate or incomplete or the amendment is otherwise warranted; in these circumstances, it is reasonable to ask the covered entity to notify certain previous recipients of the information that reliance on such information could be harmful. Where, however, the request for amendment is denied, the covered entity believes that the relevant information is accurate and complete or the amendment is otherwise unacceptable. In this circumstance, the burden of prior notification outweighs the potential benefits. We therefore do not require notification of prior recipients.

We agree, however, that individuals should know how a covered entity has responded to their requests, and therefore add a requirement that covered entities also provide a copy of any rebuttal statements to the individual.

Section 164.528—Accounting of Disclosures of Protected Health Information

Comment: Many commenters expressed support for the concept of the right to receive an accounting of disclosures. Others opposed even the concept. One commenter said that it is likely that some individuals will request an accounting of disclosures from each of his or her health care providers and payors merely to challenge the disclosures that the covered entity made.

Some commenters also questioned the value to the individual of providing the right to an accounting. One commenter stated that such a provision would be meaningless because those who deliberately perpetrate an abuse are unlikely to note their breach in a log.

Response: The final rule retains the right of an individual to receive an accounting of disclosures of protected health information. The provision serves multiple purposes. It provides a means of informing the individual as to which information has been sent to which recipients. This information, in turn, enables individuals to exercise certain other rights under the rule, such as the rights to inspection and amendment, with greater precision and ease. The accounting also allows individuals to monitor how covered entities are complying with the rule. Though covered entities who deliberately make disclosures in violation of the rule may be unlikely to note such a breach in the accounting, other covered entities may document inappropriate disclosures that they make out of ignorance and not malfeasance. The accounting will enable the individual to address such concerns with the covered entity.

We believe this approach is consistent with well-established privacy principles, with other law, and with industry standards and ethical guidelines. The July 1977 Report of the Privacy Protection Study Commission recommended that a health care provider should not disclose individually-identifiable information for certain purposes without the individual's authorization unless ''an accounting of such disclosures is kept and the individual who is the subject of the information being disclosed can find out that the disclosure has been made and to whom.'' [32] With certain exceptions, the Privacy Act (5 U.S.C. 552a) requires government agencies to ''keep an accurate accounting of * * * the date, nature, and purpose of each disclosure of a record to any person or to another agency * * * and * * * the name and address of the person or agency to whom the disclosure is made.'' The National Association of Insurance Commissioners' Health Information Privacy Model Act requires carriers to provide to individuals on request ''information regarding disclosure of that individual's protected health information that is sufficient to exercise the right to amend the information.'' We build on these standards in this final rule.

Comment: Many commenters disagreed with the NPRM's exception for treatment, payment, and health care operations. Some commenters wanted treatment, payment, and health care operations disclosures to be included in an accounting because they believed that improper disclosures of protected health information were likely to be committed by parties within the entity who have access to protected health information for treatment, payment, and health care operations related purposes. They suggested that requiring covered entities to record treatment, payment, and health care operations disclosures would either prevent improper disclosures or enable transgressions to be tracked.

One commenter reasoned that disclosures for treatment, payment, and health care operations purposes should be tracked since these disclosures would be made without the individual's consent. Others argued that if an individual's authorization is not required for a disclosure, then the disclosure should not have to be tracked for a future accounting to the individual.

One commenter requested that the provision be restated so that no accounting is required for disclosures ''compatible with or directly related to'' treatment, payment or health care operations. This comment indicated that the change would make § 164.515(a)(1) of the NPRM consistent with § 164.508(a)(2)(i)(A) of the NPRM.

Response: We do not accept the comments suggesting removing the exception for disclosures for treatment, payment, and health care operations. While including all disclosures within the accounting would provide more information to individuals about to whom their information has been disclosed, we believe that documenting all disclosures made for treatment, payment, and health care operations purposes would be unduly burdensome on entities and would result in accountings so voluminous as to be of questionable value. Individuals who seek treatment and payment expect that their information will be used and disclosed for these purposes. In many cases, under this final rule, the individual will have consented to these uses and disclosures. Thus, the additional information that would be gained from including these disclosures would not outweigh the added burdens on covered entities. We believe that retaining the exclusion of disclosures to carry out treatment, payment, and health care operations makes for a manageable accounting both from the point of view of entities and of individuals. We have conformed the language in this section with language in other sections of the rule regarding uses and disclosures to carry out treatment, payment, and health care operations. See § 164.508 and the corresponding preamble discussion regarding our decision to use this language.

Comments: A few commenters called for a record of all disclosures, including a right of access to a full audit trail where one exists. Some commenters stated while audit trails for paper records are too expensive to require, the privacy rule should not discourage audit trails, at least for computer-based records. They speculated that an important reason for maintaining a full audit trail is that most abuses are the result of activity by insiders. On the other hand, other commenters pointed out that an enormous volume of records would be created if the rule requires recording all accesses in the manner of a full audit trail.

One commenter supported the NPRM's reference to the proposed HIPAA Security Rule, agreeing that access control and disclosure requirements under this rule should be coordinated with the final HIPAA Security Rule. The commenter recommended that HHS add a reference to the final HIPAA Security Rule in this section and keep specific audit log and reporting requirements generic in the privacy rule.

Response: Audit trails and the accounting of disclosures serve different functions. In the security field, an audit trail is typically a record of each time a sensitive record is altered, how it was altered and by whom, but does not usually record each time a record is used or viewed. The accounting required by this rule provides individuals with information about to whom a disclosure is made. An accounting, as described in this rule, would not capture uses. To the extent that an audit trail would capture uses, consumers reviewing an audit trail may not be able to distinguish between

[32] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, pp. 306–307.

accesses of the protected health information for use and accesses for disclosure. Further, it is not clear the degree to which the field is technologically poised to provide audit trails. Some entities could provide audit trails to individuals upon their request, but we are concerned that many could not.

We agree that it is important to coordinate this provision of the privacy rule with the Security Rule when it is issued as a final rule.

Comments: We received many comments from researchers expressing concerns about the potential impact of requiring an accounting of disclosures related to research. The majority feared that the accounting provision would prove so burdensome that many entities would decline to participate in research. Many commenters believed that disclosure of protected health information for research presents little risk to individual privacy and feared that the accounting requirement could shut down research.

Some commenters pointed out that often only a few data elements or a single element is extracted from the patient record and disclosed to a researcher, and that having to account for so singular a disclosure from what could potentially be an enormous number of records imposes a significant burden. Some said that the impact would be particularly harmful to longitudinal studies, where the disclosures of protected health information occur over an extended period of time. A number of commenters suggested that we not require accounting of disclosures for research, registries, and surveillance systems or other databases unless the disclosure results in the actual physical release of the patient's entire medical record, rather than the disclosure of discrete elements of information contained within the record.

We also were asked by commenters to provide an exclusion for research subject to IRB oversight or research that has been granted a waiver of authorization pursuant to proposed § 164.510, to exempt ''in-house'' research from the accounting provision, and to allow covered entities to describe the type of disclosures they have made to research projects, without specifically listing each disclosure. Commenters suggested that covered entities could include in an accounting a listing of the various research projects in which they participated during the time period at issue, without regard to whether a particular individual's protected health information was disclosed to the project.

Response: We disagree with suggestions from commenters that an accounting of disclosures is not necessary for research. While it is possible that informing individuals about the disclosures made of their health information may on occasion discourage worthwhile activities, we believe that individuals have a right to know who is using their health information and for what purposes. This information gives individuals more control over their health information and a better base of knowledge from which to make informed decisions.

For the same reasons, we also do not believe that IRB or privacy board review substitutes for providing individuals the right to know how their information has been disclosed. We permit IRBs or privacy boards to determine that a research project would not be feasible if authorization were required because we understand that it could be virtually impossible to get authorization for archival research involving large numbers of individuals or where the location of the individuals is not easy to ascertain. While providing an accounting of disclosures for research may entail some burden, it is feasible, and we do not believe that IRBs or privacy boards would have a basis for waiving such a requirement. We also note that the majority of comments that we received from individuals supported including more information in the accounting, not less.

We understand that requiring covered entities to include disclosures for research in the accounting of disclosures entails some burden, but we believe that the benefits described above outweigh the burden.

We do not agree with commenters that we should exempt disclosures where only a few data elements are released or in the case of data released without individuals' names. We recognize that information other than names can identify an individual. We also recognize that even a few data elements could be clues to an individual's identity. The actual volume of information released is not an appropriate indicator of whether an individual could have a concern about privacy.

We disagree with comments that suggested that it would be sufficient to provide individuals with a general list of research projects to which information has been disclosed by the covered entity. We believe that individuals are entitled to a level of specificity about disclosures of protected health information about them and should know to which research projects their protected health information has been disclosed, rather than to which projects protected health information may have been disclosed. However, we have added a provision allowing for a summary accounting of recurrent disclosures. For multiple disclosures to the same recipient pursuant to a single authorization or for a single purpose permitted under the rule without authorization, the covered entity may provide a summary accounting addressing the series of disclosures rather than a detailed accounting of each disclosure in the series. This change is designed to ease the burden on covered entities involved in longitudinal projects.

With regard to the suggestion that we exempt ''in-house'' research from the accounting provision, we note that only disclosures of protected health information must appear in an accounting.

Comments: Several commenters noted that disclosures for public health activities may be of interest to individuals, but add to the burden imposed on entities. Furthermore, some expressed fear that priority public health activities would be compromised by the accounting provision. One commenter from a health department said that covered entities should not be required to provide an accounting to certain index cases, where such disclosures create other hazards, such as potential harm to the reporting provider. This commenter also speculated that knowing protected health information had been disclosed for these public health purposes might cause people to avoid treatment in order to avoid being reported to the public health department.

A provider association expressed concern about the effect that the accounting provision might have on a non-governmental, centralized disease registry that it operates. The provider organization feared that individuals might request that their protected health information be eliminated in the databank, which would make the data less useful.

Response: As in the discussion of research above, we reject the contention that we should withhold information from individuals about where their information has been disclosed because informing them could occasionally discourage some worthwhile activities. We also believe that, on balance, individuals' interest in having broad access to this information outweighs concerns about the rare instances in which providing this information might raise concerns about harm to the person who made the disclosure. As we stated above, we believe that individuals have

a right to know who is using their health information and for what purposes. This information gives individuals more control over their health information and a better base of knowledge from which to make informed decisions.

Comment: We received many comments about the proposed time-limited exclusion for law enforcement and health oversight. Several commenters noted that it is nearly impossible to accurately project the length of an investigation, especially during its early stages. Some recommended we permit a deadline based on the end of an event, such as conclusion of an investigation. One commenter recommended amending the standard such that covered entities would never be required to give an accounting of disclosures to health oversight or law enforcement agencies. The commenter noted that there are public policy reasons for limiting the extent to which a criminal investigation is made known publicly, including the possibility that suspects may destroy or falsify evidence, hide assets, or flee. The commenter also pointed out that disclosure of an investigation may unfairly stigmatize a person or entity who is eventually found to be innocent of any wrongdoing.

On the other hand, many commenters disagreed with the exemption for recording disclosures related to oversight activities and law enforcement. Many of these commenters stated that the exclusion would permit broad exceptions for government purposes while holding disclosures for private purposes to a more burdensome standard.

Some commenters felt that the NPRM made it too easy for law enforcement to obtain an exception. They suggested that law enforcement should not be excepted from the accounting provision unless there is a court order. One commenter recommended that a written request for exclusion be dated, signed by a supervisory official, and contain a certification that the official is personally familiar with the purpose of the request and the justification for exclusion from accounting.

Response: We do not agree with comments suggesting that we permanently exclude disclosures for oversight or law enforcement from the accounting. We believe generally that individuals have a right to know who is obtaining their health information and for what purposes.

At the same time, we agree with commenters that were concerned that an accounting could tip off subjects of investigations. We have retained a time-limed exclusion period similar to that proposed in the NPRM. To protect the integrity of investigations, in the final rule we require covered entities to exclude disclosures to a health oversight agency or law enforcement official for the time specified by that agency or official, if the agency or official states that including the disclosure in an accounting to the individual would be reasonably likely to impede the agency or official's activities. We require the statement from the agency or official to provide a specific time frame for the exclusion. For example, pursuant to a law enforcement official's statement, a covered entity could exclude a law enforcement disclosure from the accounting for a period of three months from the date of the official's statement or until a date specified in the statement.

In the final rule, we permit the covered entity to exclude the disclosure from an accounting to an individual if the agency or official makes the statement orally and the covered entity documents the statement and the identify of the agency or official that made the statement. We recognize that in urgent situations, agencies and officials may not be able to provide statements in writing. If the agency or official's statement is made orally, however, the disclosure can be excluded from an accounting to the individual for no longer than 30 days from the oral statement. For exclusions longer than 30 days, a covered entity must receive a written statement.

We believe these requirements appropriately balance individuals' rights to be informed of the disclosures of protected health information while recognizing the public's interest in maintaining the integrity of health oversight and law enforcement activities.

Comment: One commenter stated that under Minnesota law, providers who are mandated reporters of abuse are limited as to whom they may reveal the report of abuse (generally law enforcement authorities and other providers only). This is because certain abusers, such as parents, by law may have access to a victim's (child's) records. The commenter requested clarification as to whether these disclosures are exempt from the accounting requirement or whether preemption would apply.

Response: While we do not except mandatory disclosures of abuse from the accounting for disclosure requirement, we believe the commenter's concerns are addressed in several ways. First, nothing in this regulation invalidates or limits the authority or procedures established under state law providing for the reporting of child abuse. Thus, with respect to child abuse the Minnesota law's procedures are not preempted even though they are less stringent with respect to privacy. Second, with respect to abuse of persons other than children, we allow covered entities to refuse to treat a person as an individual's personal representative if the covered entity believes that the individual has been subjected to domestic violence, abuse, or neglect from the person. Thus, the abuser would not have access to the accounting. We also note that a covered entity must exclude a disclosure, including disclosures to report abuse, from the accounting for specified period of time if the law enforcement official to whom the report is made requests such exclusion.

Comment: A few comments noted the lack of exception for disclosures made to intelligence agencies.

Response: We agree with the comments and have added an exemption for disclosures made for national security or intelligence purposes under § 164.512(k)(2). Individuals do not have a right to an accounting of disclosures for these purposes.

Comment: Commenters noted that the burden associated with this provision would, in part, be determined by other provisions of the rule, including the definitions of ''individually identifiable,'' ''treatment,'' and ''health care operations.'' They expressed concern that the covered entity would have to be able to organize on a patient by patient basis thousands of disclosures of information, which they described as ''routine.'' These commenters point to disclosures for patient directory information, routine banking and payment processes, uses and disclosures in emergency circumstances, disclosures to next of kin, and release of admissions statistics to a health oversight agency.

Response: We disagree with the commenters that ambiguity in other areas of the rule increase the burden associated with maintaining an accounting. The definitions of treatment, payment, and health operations are necessarily broad and there is no accounting required for disclosures for these purposes. These terms cover the vast majority of routine disclosures for health care purposes. (See § 164.501 and the associated preamble for a discussion of changes made to these definitions.)

The disclosures permitted under § 164.512 are for national priority purposes, and determining whether a disclosure fits within the section is necessary before the disclosure can be

made. There is no additional burden, once such a determination is made, in determining whether it must be included in the accounting.

We agree with the commenters that there are areas where we can reduce burden by removing additional disclosures from the accounting requirement, without compromising individuals' rights to know how their information is being disclosed. In the final rule, covered entities are not required to include the following disclosures in the accounting: disclosures to the individual, disclosures for facility directories under § 164.510(a), or disclosures to persons assisting in the individual's care or for other notification purposes under § 164.510(b). For each of these types of disclosures, the individual is likely to already know about the disclosure or to have agreed to the disclosure, making the inclusion of such disclosures in the accounting less important to the individual and unnecessarily burdensome to the covered entity.

Comment: Many commenters objected to requiring business partners to provide an accounting to covered entities upon their request. They cited the encumbrance associated with re-contracting with the various business partners, as well as the burden associated with establishing this type of record keeping.

Response: Individuals have a right to know to whom and for what purpose their protected health information has been disclosed by a covered entity. The fact that a covered entity uses a business associate to carry out a function does not diminish an individual's right to know.

Comments: One commenter requested clarification as to how far a covered entity's responsibility would extend, asking whether an entity had to track only their direct disclosures or subsequent re-disclosures.

Response: Covered entities are required to account for their disclosures, as well as the disclosures of their business associates, of protected health information. Because business associates act on behalf of covered entities, it is essential that their disclosures be included in any accounting that an individual requests from a covered entity. Covered entities are not responsible, however, for the actions of persons who are not their business associates. Once a covered entity has accounted for a disclosure to any person other than a business associate, it is not responsible for accounting for any further uses or disclosures of the information by that other person.

Comments: Some commenters said that the accounting provision described in the NPRM was ambiguous and created uncertainty as to whether it addresses disclosures only, as the title would indicate, or whether it includes accounting of uses. They urged that the standard address disclosures only, and not uses, which would make implementation far more practicable and less burdensome.

Response: The final rule requires disclosures, not uses, to be included in an accounting. See § 164.501 for definitions of ''use'' and ''disclosure.''

Comments: We received many comments from providers and other representatives of various segments of the health care industry, expressing the view that a centralized system of recording disclosures was not possible given the complexity of the health care system, in which disclosures are made by numerous departments within entities. For example, commenters stated that a hospital medical records department generally makes notations regarding information it releases, but that these notations do not include disclosures that the emergency department may make. Several commenters proposed that the rule provide for patients to receive only an accounting of disclosures made by medical records departments or some other central location, which would relieve the burden of centralizing accounting for those entities who depend on paper records and tracking systems.

Response: We disagree with commenters' arguments that covered entities should not be held accountable for the actions of their subdivisions or workforce members. Covered entities are responsible for accounting for the disclosures of protected health information made by the covered entity, in accordance with this rule. The particular person or department within the entity that made the disclosure is immaterial to the covered entity's obligation. In the final rule, we require covered entities to document each disclosure that is required to be included in an accounting. We do not, however, require this documentation to be maintained in a central registry. A covered hospital, for example, could maintain separate documentation of disclosures that are made from the medical records department and the emergency department. At the time an individual requests an accounting, this documentation could be integrated to provide a single accounting of disclosures made by the covered hospital. Alternatively, the covered hospital could centralize its processes for making and documenting disclosures. We believe this provision provides covered entities with sufficient flexibility to meet their business needs without compromising individuals' rights to know how information about them is disclosed.

Comments: Commenters stated that the accounting requirements placed undue burden on covered entities that use paper, rather than electronic, records.

Response: We do not agree that the current reliance on paper records makes the accounting provision unduly burdensome. Covered entities must use the paper records in order to make a disclosure, and have the opportunity when they do so to make a notation in the record or in a separate log. We require an accounting only for disclosures for purposes other than treatment, payment, and health care operations. Such disclosures are not so numerous that they cannot be accounted for, even if paper records are involved.

Comments: The exception to the accounting provision for disclosures of protected health information for treatment, payment, and health care operations purposes was viewed favorably by many respondents. However, at least one commenter stated that since covered entities must differentiate between disclosures that require documentation and those that do not, they will have to document each instance when a patient's medical record is disclosed to determine the reason for the disclosure. This commenter also argued that the administrative burden of requiring customer services representatives to ask in which category the information falls and then to keep a record that they asked the question and record the answer would be overwhelming for plans. The commenter concluded that the burden of documentation on a covered entity would not be relieved by the stipulation that documentation is not required for treatment, payment, and health care operations.

Response: We disagree. Covered entities are not required to document every disclosure in order to differentiate those for treatment, payment, and health care operations from those for purposes for which an accounting is required. We require that, when a disclosure is made for which an accounting is required, the covered entity be able to produce an accounting of those disclosures upon request. We do not require a covered entity to be able to account for every disclosure. In addition, we believe that we have addressed many of the commenters' concerns by clarifying in the final rule that disclosures to the

individual, regardless of the purpose for the disclosure, are not subject to the accounting requirement.

Comments: An insurer explained that in the context of underwriting, it may have frequent and multiple disclosures of protected health information to an agent, third party medical provider, or other entity or individual. It requested we reduce the burden of accounting for such disclosures.

Response: We add a provision allowing for a summary accounting of recurrent disclosures. For multiple disclosures to the same recipient pursuant to a single authorization or for a single purpose permitted under the rule without authorization, the covered entity may provide a summary accounting addressing the series of disclosures rather than a detailed accounting of each disclosure in the series.

Comment: Several commenters said that it was unreasonable to expect covered entities to track disclosures that are requested by the individual. They believed that consumers should be responsible for keeping track of their own requests.

Other commenters asked that we specify that entities need not retain and provide copies of the individual's authorization to disclose protected health information. Some commenters were particularly concerned that if they maintain all patient information on a computer system, it would be impossible to link the paper authorization with the patient's electronic records.

Another commenter suggested we allow entities to submit copies of authorizations after the 30-day deadline for responding to the individual, as long as the accounting itself is furnished within the 30-day window.

Response: In the final rule we do not require disclosures to the individual to be included in the accounting. Other disclosures requested by the individual must be included in the accounting, unless they are otherwise excepted from the requirement. We do not agree that individuals should be required to track these disclosures themselves. In many cases, an authorization may authorize a disclosure by more than one entity, or by a class of entities, such as all physicians who have provided medical treatment to the individual. Absent the accounting, the individual cannot know whether a particular covered entity has acted on the authorization.

We agree, however, that it is unnecessarily burdensome to require covered entities to provide the individual with a copy of the authorization. We remove the requirement. Instead, we require the accounting to contain a brief statement describing the purpose for which the protected health information was disclosed. The statement must be sufficient to reasonably inform the individual of the basis for the disclosure. Alternatively, the covered entity may provide a copy of the authorization or a copy of the written request for disclosure, if any, under §§ 164.502(a)(2)(ii) or 164.512.

Comments: We received many comments regarding the amount of information required in the accounting. A few commenters requested that we include additional elements in the accounting, such as the method of transmittal and identity of the employee who accessed the information.

Other commenters, however, felt that the proposed requirements went beyond what is necessary to inform the individual of disclosures. Another commenter stated that if the individual's right to obtain an accounting extends to disclosures that do not require a signed authorization, then the accounting should be limited to a disclosure of the manner and purpose of disclosures, as opposed to an individual accounting of each entity to whom the protected health information was disclosed. An insurer stated that this section of the proposed rule should be revised to provide more general, rather than detailed, guidelines for accounting of disclosures. The commenter believed that its type of business should be allowed to provide general information regarding the disclosure of protected health information to outside entities, particularly with regard to entities with which the insurer maintains an ongoing, standard relationship (such as a reinsurer).

Response: In general, we have retained the proposed approach, which we believe strikes an appropriate balance between the individual's right to know to whom and for what purposes their protected health information has been disclosed and the burden placed on covered entities. In the final rule, we clarify that the accounting must include the address of the recipient only if the address is known to the covered entity. As noted above, we also add a provision allowing for a summary accounting of recurrent disclosures. We note that some of the activities of concern to commenters may fall under the definition of health care operations (see § 164.501 and the associated preamble).

Comment: A commenter asked that we limit the accounting to information pertaining to the medical record itself, as opposed to protected health information more generally. Similarly, commenters suggested that the accounting be limited to release of the medical record only.

Response: We disagree. Protected health information exists in many forms and resides in many sources. An individual's right to know to whom and for what purposes his or her protected health information has been disclosed would be severely limited if it pertained only to disclosure of the medical record, or information taken only from the record.

Comment: A commenter asked that we make clear that only disclosures external to the organization are within the accounting requirement.

Response: We agree. The requirement only applies to disclosures of protected health information, as defined in § 164.501.

Comment: Some commenters requested that we establish a limit on the number of times an individual could request an accounting. One comment suggested we permit individuals to request one accounting per year; another suggested two accountings per year, except in ''emergency situations.'' Others recommended that we enable entities to recoup some of the costs associated with implementation by allowing the entity to charge for an accounting.

Response: We agree that covered entities should be able to defray costs of excessive requests. The final rule provides individuals with the right to receive one accounting without charge in a twelve-month period. For additional requests by an individual within a twelve-month period, the covered entity may charge a reasonable, cost-based fee. If it imposes such a fee, the covered entity must inform the individual of the fee in advance and provide the individual with an opportunity to withdraw or modify the request to avoid or reduce the fee.

Comment: In the NPRM, we solicited comments on the appropriate duration of the individual's right to an accounting. Some commenters supported the NPRM's requirement that the right exist for as long as the covered entities maintains the protected health information. One commenter, however, noted that most audit control systems do not retain data on activity for indefinite periods of time.

Other commenters noted that laws governing the length of retention of clinical records vary by state and by provider type and suggested that entities be allowed to adhere to state laws or policies established by professional organizations or accrediting bodies. Some commenters suggested that the

language be clarified to state that whatever minimum requirements are in place for the record should also guide covered entities in retaining their capacity to account for disclosures over that same time, but no longer.

Several commenters asked us to consider specific time limits. It was pointed out that proposed § 164.520(f)(6) of the NPRM set a six-year time limit for retaining certain information including authorization forms and contracts with business partners. Included in this list was the accounting of disclosures, but this requirement was inconsistent with the more open-ended language in § 164.515. Commenters suggested that deferring to this six-year limit would make this provision consistent with other record retention provisions of the standard and might relieve some of the burden associated with implementation. Other specific time frames suggested were two years, three years, five years, and seven years.

Another option suggested by commenters was to keep the accounting record for as long as entities have the information maintained and ''active'' on their systems. Information permanently taken off the covered entity's system and sent to ''dead storage'' would not be covered. One commenter further recommended that we not require entities to maintain records or account for prior disclosures for members who have ''disenrolled.''

Response: We agree with commenters who suggested we establish a specific period for which an individual may request an accounting. In the final rule, we provide that individuals have a right to an accounting of the applicable disclosures that have been made in the six-year period prior to a request for an accounting. We adopt this time frame to conform with the other documentation retention requirements in the rule. We also note that an individual may request, and a covered entity may then provide, an accounting of disclosures for a period of time less than six years from the date of the request. For example, an individual could request an accounting only of disclosures that occurred during the year prior to the request. In addition, we note that covered entities do not have to account for disclosures that occurred prior to the compliance date of this rule.

Comments: Commenters asked that we provide more time for entities to respond to requests for accounting. Suggestions ranged from 60 days to 90 days. Another writer suggested that entities be able to take up to three 30-day extensions from the original 30-day deadline. Commenters raised concerns about the proposed requirement that a covered health care provider or health plan act as soon as possible.

Response: We agree with concerns raised by commenters and in the final rule, covered entities are required to provide a requested accounting no later than 60 days after receipt of the request. We also provide for one 30 day extension if the covered entity is unable to provide the accounting within the standard time frame. We eliminate the requirement for a covered entity to act as soon as possible.

We recognize that circumstances may arise in which an individual will request an accounting on an expedited basis. We encourage covered entities to implement procedures for handling such requests. The time limitation is intended to be an outside deadline, rather than an expectation. We expect covered entities always to be attentive to the circumstances surrounding each request and to respond in an appropriate time frame.

Comment: A commenter asked that we provide an exemption for disclosures related to computer upgrades, when protected health information is disclosed to another entity solely for the purpose of establishing or checking a computer system.

Response: This activity falls within the definition of health care operations and is, therefore, excluded from the accounting requirement.

Section 164.530—Administrative Requirements

Section 164.530(a)—Designation of a Privacy Official and Contact Person

Comment: Many of the commenters on this topic objected to the cost of establishing a privacy official, including the need to hire additional staff, which might need to include a lawyer or other highly paid individual.

Response: We believe that designation of a privacy official is essential to ensure a central point of accountability within each covered entity for privacy-related issues. The privacy official is charged with developing and implementing the policies and procedures for the covered entity, as required throughout the regulation, and for compliance with the regulation generally. While the costs for these activities are part of the costs of compliance with this rule, not extra costs associated with the designation of a privacy official, we do anticipate that there will be some cost associated with this requirement. The privacy official role may be an additional responsibility given to an existing employee in the covered entity, such as an office manager in a small entity or an information officer or compliance official in a larger institution. Cost estimates for the privacy official are discussed in detail in the overall cost analysis.

Comment: A few commenters argued for more flexibility in meeting the requirement for accountability. One health care provider maintained that covered entities should be able to establish their own system of accountability. For example, most physician offices already have the patient protections incorporated in the proposed administrative requirements—the commenter urged that the regulation should explicitly promote the application of flexibility and scalability. A national physician association noted that, in small offices, in particular, responsibility for the policies and procedures should be allowed to be shared among several people. A major manufacturing corporation asserted that mandating a privacy official is unnecessary and that it would be preferable to ask for the development of policies that are designed to ensure that processes are maintained to assure compliance.

Response: We believe that a single focal point is needed to achieve the necessary accountability. At the same time, we recognize that covered entities are organized differently and have different information systems. We therefore do not prescribe who within a covered entity must serve as the privacy official, nor do we prohibit combining this function with other duties. Duties may be delegated and shared, so long as there is one point of accountability for the covered entity's policies and procedures and compliance with this regulation.

Comment: Some commenters echoed the proposal of a professional information management association that the regulation establish formal qualifications for the privacy official, suggesting that this should be a credentialed information management professional with specified minimum training standards. One commenter emphasized that the privacy official should be sufficiently high in management to have influence.

Response: While there may be some advantages to establishing formal qualifications, we concluded the disadvantages outweigh the advantages. Since the job of privacy official will differ substantially among organizations of varying size and function, specifying a single set of qualifications would sacrifice flexibility and scalability in implementation.

Comment: A few commenters suggested that we provide guidance on the tasks of the privacy official. One noted that this would reduce the burden on covered entities to clearly identify those tasks during the initial HIPAA implementation phase.

Response: The regulation itself outlines the tasks of the privacy official, by specifying the policies and procedures required, and otherwise explaining the duties of covered entities. Given the wide variation in the function and size of covered entities, providing further detail here would unnecessarily reduce flexibility for covered entities. We will, however, provide technical assistance in the form of guidance on the various provisions of the regulation before the compliance date.

Comment: Some comments expressed concern that the regulation would require a company with subsidiaries to appoint a privacy official within each subsidiary. Instead they argued that the corporate entity should have the option of designating a single corporate official rather than one at each subsidiary.

Response: In the final regulation, we give covered entities with multiple subsidiaries that meet the definition of covered entities under this rule the flexibility to designate whether such subsidiaries are each a separate covered entity or are together a single covered entity. (See § 164.504(b) for the rules requiring such designation.) If only one covered entity is designated for the subsidiaries, only one privacy officer is needed. Further, we do not prohibit the privacy official of one covered entity from serving as the privacy official of another covered entity, so long as all the requirements of this rule are met for each such covered entity.

Section 164.530(b)—Training

Comment: A few commenters felt that the proposed provision was too stringent, and that the content of the training program should be left to the reasonable discretion of the covered entity.

Response: We clarify that we do not prescribe the content of the required training; the nature of the training program is left to the discretion of the covered entity. The scenarios in the NPRM preamble of potential approaches to training for different sized covered entities were intended as examples of the flexibility and scalability of this requirement.

Comment: Most commenters on this provision asserted that recertification/retraining every three years is excessive, restrictive, and costly. Commenters felt that retraining intervals should be left to the discretion of the covered entity. Some commenters supported retraining only in the event of a material change. Some commenters supported the training requirement as specified in the NPRM.

Response: For the reasons cited by the commenters, we eliminate the triennial recertification requirements in the final rule. We also clarify that retraining is not required every three years. Retraining is only required in the case of material changes to the privacy policies and procedures of the covered entity.

Comment: Several commenters objected to the burden imposed by required signatures from employees after they are trained. Many commenters suggested that electronic signatures be accepted for various reasons. Some felt that it would be less costly than manually producing, processing, and retaining the hard copies of the forms. Some suggested sending out the notice to the personal workstation via email or some other electronic format and having staff reply via email. One commenter suggested that the covered entity might opt to give web based training instead of classroom or some other type. The commenter indicated that with web based training, the covered entity could record whether or not an employee had received his or her training through the use of a guest book or registration form on the web site. Thus, a physical signature should not be required.

Response: We agree that there are many appropriate mechanisms by which covered entities can implement their training programs, and therefore remove this requirement for signature. We establish only a general requirement that covered entities document compliance with the training requirement.

Comment: Some commenters were concerned that there was no proposed requirement for business associates to receive training and/or to train their employees. The commenters believed that if the business associate violated any privacy requirements, the covered entity would be held accountable. These commenters urged the Secretary to require periodic training for appropriate management personnel assigned outside of the component unit of the covered entity, including business associates. Other commenters felt that it would not be fair to require covered entities to impose training requirements on business associates.

Response: We do not have the statutory authority directly to require business associates to train their employees. We also believe it would be unnecessarily burdensome to require covered entities to monitor business associates' establishment of specific training requirements. Covered entities' responsibility for breaches of privacy by their business associates is described in §§ 164.504(e) and 164.530(f). If a covered entity believes that including a training requirement in one or more of its business associate contracts is an appropriate means of protecting the health information provided to the business associate, it is free to do so.

Comments: Many commenters argued that training, as well as all of the other administrative requirements, are too costly for covered entities and that small practices would not be able to bear the added costs. Commenters also suggested that HHS should provide training materials at little, or no, cost to the covered entity.

Response: For the final regulation, we make several changes to the proposed provisions. We believe that these changes address the issue of administrative cost and burden to the greatest extent possible, consistent with protecting the privacy of health information. In enforcing the privacy rule, we expect to provide general training materials. We also hope to work with professional associations and other groups that target classes of providers, plans and patients, in developing specialized material for these groups.

We note that, under long-standing legal principles, entities are generally responsible for the actions of their workforce. The requirement to train workforce members to implement the covered entity's privacy policies and procedures, and do such things as pass evidence of potential problems to those responsible, is in line with these principles. For example, the comments and our fact finding indicate that, today, many hospitals require their workforce members to sign a confidentiality agreement, and include confidentiality matters in their employee handbooks.

Section 164.530(c)—Safeguards

Comments: A few comments assert that the rule requires some institutions that do not have adequate resources to develop costly physical and technical safeguards without providing a funding mechanism to do so. Another comment said that the vague definitions of adequate and appropriate safeguards could be interpreted by HHS to require the purchase of new computer systems and reprogram many old ones. A few other comments suggested that the safeguards language was vague and asked for more specifics.

Response: We require covered entities to maintain safeguards adequate for their operations, but do not require that

specific technologies be used to do so. Safeguards need not be expensive or high-tech to be effective. Sometimes, it is an adequate safeguard to put a lock on a door and only give the keys to those who need access. As described in more detail in the preamble discussion of § 164.530, we do not require covered entities to guarantee the safety of protected health information against all assaults. This requirement is flexible and scalable to allow implementation of required safeguards at a reasonable cost.

Comments: A few commenters noted that once protected health information becomes non-electronic, by being printed for example, it escapes the protection of the safeguards in the proposed Security Rule. They asked if this safeguards requirement is intended to install similar security protections for non-electronic information.

Response: This provision is not intended to incorporate the provisions in the proposed Security regulation into this regulation, or to otherwise require application of those provisions to paper records.

Comments: Some commenters said that it was unclear what ''appropriate'' safeguards were required by the rule and who establishes the criteria for them. A few noted that the privacy safeguards were not exactly the same as the security safeguards, or that the ''other safeguards'' section was too vague to implement. They asked for more clarification of safeguards requirements and flexible solutions.

Response: In the preamble discussion of § 164.530, we provide examples of types of safeguards that can be appropriate to satisfy this requirement. Other sections of this regulation require specific safeguards for specific circumstances. The discussion of the requirements for ''minimum necessary'' uses and disclosures of protected health information includes related guidance for developing role-based access policies for a covered entity's workforce. The requirements for ''component entities'' include requirements for firewalls to prevent access by unauthorized persons. The proposed Security Rule included further details on what safeguards would be appropriate for electronic information systems. The flexibility and scalability of these rules allows covered entities to analyze their own needs and implement solutions appropriate for their own environment.

Comments: A few comments asked for a requirement for a firewall between a health care component and the rest of a larger organization as another appropriate safeguard.

Response: We agree, and have incorporated such a requirement in § 164.504.

Comments: One commenter agreed with the need for administrative, physical, and technical safeguards, but took issue with our specification of the type of documentation or proof that the covered entity is taking action to safeguard protected health information.

Response: This privacy rule does not require specific forms of proof for safeguards.

Comments: A few commenters asked that, for the requirement for a signed certification of training and the requirements for verification of identity, we consider the use of electronic signatures that meet the requirements in the proposed security regulation to meet the requirements of this rule.

Response: In this final rule, we drop the requirements for signed certifications of training. Signatures are required elsewhere in this regulation, for example, for a valid authorization. In the relevant sections we clarify that electronic signatures are sufficient provided they meet standards to be adopted under HIPAA. In addition, we do not intend to interfere with the application of the Electronic Signature in Global and National Commerce Act.

Comments: A few commenters requested that the privacy requirements for appropriate administrative, technical, and physical safeguards be considered to have been met if the requirements of the proposed Security Rule have been met. Others requested that the safeguards requirements of the final Privacy Rule mirror or be harmonized with the final Security Rule so they do not result in redundant or conflicting requirements.

Response: Unlike the proposed regulation, the final regulation covers all protected health information, not just information that had at some point been electronic. Thus, these commenters' assumption that the proposed Privacy Rule and the proposed Security Rule covered the same information is not the case, and taking the approach suggested by these comments would leave a significant number of health records unprotected. The safeguards required by this regulation are appropriate for both paper and electronic information. We will take care to ensure that the final Security Rule works in tandem with these requirements.

Comments: One commenter requested that the final privacy rule be published before the final Security Rule, recognizing that the privacy policies must be in place before the security technology used to implement them could be worked out. Another commenter asked that the final Security Rule be published immediately and not wait for an expected delay while privacy policies are worked out.

Response: Now that this final privacy rule has been published in a timely manner, the final Security Rule can be harmonized with it and published soon.

Comments: Several commenters echoed an association recommendation that, for those organizations that have implemented a computer based patient record that is compliant with the requirements of the proposed Security Rule, the minimum necessary rule should be considered to have been met by the implementation of role-based access controls.

Response: The privacy regulation applies to paper records to which the proposed Security Rule does not apply. Thus, taking the approach suggested by these comments would leave a significant number of health records unprotected. Further, since the final Security Rule is not yet published and the number of covered entities that have implemented this type of computer-based patient record systems is still small, we cannot make a blanket statement. We note that this regulation requires covered entities to develop role-based access rules, in order to implement the requirements for ''minimum necessary'' uses and disclosures of protected health information. Thus, this regulation provides a foundation for the type of electronic system to which these comments refer.

Section 164.530(d)—Complaints to the Covered Entity

Comment: Several commenters felt that some form of due process is needed when it comes to internal complaints. Specifically, they wanted to be assured that the covered entity actually hears the complaints made by the individual and that the covered entity resolves the complaint within a reasonable time frame. Without due process the commenters felt that the internal complaint process is open ended. Some commenters wanted the final rule to include an appeals process for individuals if a covered entity's determination in regards to the complaint is unfavorable to the individual.

Response: We do not require covered entities to implement any particular due process or appeals process for complaints, because we are concerned about the burden this could impose on covered entities. We provide individuals with an alternative to take their complaints to the Secretary. We believe that this provides incentives for

covered entities to implement a complaint process that resolves complaints to individuals' satisfaction.

Comment: Some commenters felt that the individual making the complaint should exhaust all other avenues to resolve their issues before filing a complaint with the Secretary. A number of commenters felt that any complaint being filed with the Secretary should include documentation of the reviews done by the covered entity.

Response: We reject these suggestions, for two reasons. First, we want to avoid establishing particular process requirements for covered entities' complaint programs. Also, this rule does not require the covered entity to share any information with the complainant, only to document the receipt of the complaint and the resolution, if any. Therefore, we cannot expect the complainant to have this information available to submit to the Secretary. Second, we believe the individual making the complaint should have the right to share the complaint with the Secretary at any point in time. This approach is consistent with existing civil rights enforcement programs for which the Department is responsible. Based on that experience, we believe that most complaints will come first to covered entities for disposition.

Comment: Some commenters wanted the Department to prescribe a minimum amount of time before the covered entity could dispose of the complaints. They felt that storing these complaints indefinitely would be cumbersome and expensive.

Response: We agree, and in the final rule require covered entities to keep all items that must be documented, including complaints, for at least six years from the date of creation.

Comments: Some commenters objected to the need for covered entities to have at least one employee, if not more, to deal with complaints. They felt that this would be costly and is redundant in light of the designation of a contact person to receive complaints.

Response: We do not require assignment of dedicated staff to handle complaints. The covered entity can determine staffing based on its needs and business practices. We believe that consumers need one clear point of contact for complaints, in order that this provision effectively inform consumers how to lodge complaints and so that the compliant will get to someone who knows how to respond. The contact person (or office) is for receipt of complaints, but need not handle the complaints.

Section 164.530(e)—Sanctions

Comment: Commenters argued that most covered entities already have strict sanctions in place for violations of a patient's privacy, either due to current laws, contractual obligations, or good operating practices. Requiring covered entities to create a formal sanctioning process would be superfluous.

Response: We believe it is important for the covered entity to have these sanction policies and procedures documented so that employees are aware of what actions are prohibited and punishable. For entities that already have sanctions policies in place, it should not be problematic to document those policies. We do not define the particular sanctions that covered entities must impose.

Comment: Several commenters agreed that training should be provided and expectations should be clear so that individuals are not sanctioned for doing things that they did not know were wrong or inappropriate. A good faith exception should be included in the final rule to protect these individuals.

Response: We agree that employees should be trained to understand the covered entity's expectations and understand the consequences of any violation. This is why we are requiring each covered entity to train its workforce. However, we disagree that a good faith exception is explicitly needed in the final rule. We leave the details of sanctions policies to the discretion of the covered entity. We believe it is more appropriate to leave this judgment to the covered entity that will be familiar with the circumstances of the violation, rather than to specify such requirements in the regulation.

Comment: Some commenters felt that the sanctions need to reach business partners as well, not just employees of the covered entities. These commenters felt all violators should be sanctioned, including government officials and agencies.

Response: All members of a covered entity's workforce are subject to sanctions for violations, including government officials who are part of a covered entity's workforce. Requirements for addressing privacy violations by business associates are discussed in §§ 164.504(e) and 164.530(f).

Comments: Many commenters appreciated the flexibility left to the covered entities to determine sanctions. However, some were concerned that the covered entity would need to predict each type of violation and the associated sanction. They argue that, if the Department could not determine this in the NPRM, then the covered entities should be allowed to come up with sanctions as appropriate at the time of the violation. Some commenters wanted a better explanation and understanding of what HHS' expectation is of when is it appropriate to apply sanctions. Some commenters felt that the sanctioning requirement is nebulous and requires independent judgment of compliance; as a result it is hard to enforce. Offending individuals may use the vagueness of the standard as an defense.

Response: We agree with the commenters that argue that covered entities should be allowed to determine the specific sanctions as appropriate at the time of the violation. We believe it is more appropriate to leave this judgment to the covered entity, because the covered entity will be familiar with the circumstances of the violation and the best way to improve compliance.

Comment: A commenter felt that the self-imposition of this requirement is an inadequate protection, as there is an inherent conflict of interest when an entity must sanction one of its own.

Response: We believe it is in the covered entity's best interests to appropriately sanction those individuals who do not follow the outlined policies and procedures. Allowing violations to go unpunished may lead bigger problems later, and result in complaints being registered with the Department by aggrieved parties and/or an enforcement action.

Comment: This provision should cover all violations, not just repeat violations.

Response: We do not limit this requirement to repeat offenses.

Section 164.530(f)—Duty To Mitigate

Comments: A few commenters felt that any duty to mitigate would be onerous, especially for small entities. One commenter supported an affirmative duty to mitigate for employees of the covered entity, as long as there is no prescribed mitigation policy. One commenter stated that a requirement for mitigation is unnecessary because any prudent entity would do it.

Some practitioner organizations as well as a health plan, expressed concern about the obligation to mitigate in the context of the business associate relationship. Arguing that it is unnecessary for the regulation to explicitly extend the duty to mitigate to business associates, commenters noted that: Any prudent entity would discipline a vendor or employee that violates a regulation; that the matter is best left to the terms of the contract, and that it is difficult and expensive for a

business associate to have a separate set of procedures on mitigation for each client/provider. One commenter suggested that the federal government should fund the monitoring needed to administer the requirement.

Response: Eliminating the requirement to mitigate harm would undermine the purposes of this rule by reducing covered entities' accountability to their patients for failure to protect their confidential data. To minimize burden, we do not prescribe what mitigation policies and procedures must be implemented. We require only that the covered entity mitigate harm. We also assume that violations will be rare, and so the duty to mitigate harm will rarely be triggered. To the extent a covered entity already has methods for mitigating harm, this rule will not pose significant burden, since we don't require the covered entity to follow any prescribed method or set of rules.

We also modify the NPRM to impose the duty to mitigate only where the covered entity has actual knowledge of harm. Further reducing burden, the rule requires mitigation ''to the extent practicable.'' It does not require the covered entity to eliminate the harm unless that is practicable. For example, if protected health information is advertently provided to a third party without authorization in a domestic abuse situation, the covered entity would be expected to promptly contact the patient as well as appropriate authorities and apprize them of the potential danger.

The harm to the individual is the same, whether the privacy breach was caused by a member of the covered entity's workforce, or by a contractor. We believe the cost of this requirement to be minimal for covered entities that engage in prudent business practices for exchanging protected health information with their business associates.

Comment: A few commenters noted that it is difficult to determine whether a violation has resulted in a deleterious effect, especially as the entity cannot know all places to which information has gone and uses that have been made of it. Consequently, there should be a duty to mitigate even if a deleterious effect cannot be shown, because the individual has no other redress.

Response: As noted above, this provision only applies if the covered entity has actual knowledge of the harm, and requires mitigation ''to the extent practicable.'' The covered entity is expected to take reasonable steps based on knowledge of where the information has been disclosed, how it might be used to cause harm to the patient or another individual, and what steps can actually have a mitigating effect in that specific situation.

Comments: Commenters stated that the language of the regulation was in some places vague and imprecise thus providing covered entities with insufficient guidance and allowing variation in interpretation. Commenters also noted that this could result in inconsistency in implementation as well as permitting such inconsistency to be used as a defense by an offending entity. Particular language for which at least one commenter requested clarification included ''reasonable steps'' and what is entailed in the duty to mitigate.

Response: We considered ways in which we might increase specificity, including defining ''to the extent practicable'' and ''reasonable steps'' and relating the mitigating action to the deleterious impact. While this approach could remove from the covered entity the burden of decision-making about actions that need to be taken, we believe that other factors outweighed this potential benefit. Not only would there be a loss of desirable flexibility in implementation, but it would not be possible to define ''to the extent practicable'' in a way that makes sense for all types of covered entities. We believe that allowing flexibility and judgment by those familiar with the circumstances to dictate the approach is the best approach to mitigating harm.

Section 164.530(g)—Refraining From Intimidating or Retaliatory Acts

Comment: Several commenters stated that the regulation should prohibit covered entities from engaging in intimidating or retaliatory acts against any person, not just against the ''individual,'' as proposed. They suggested adding ''or other person or entity'' after ''any individual.''

Response: We agree, and allow any person to file a compliant with the Secretary. ''Person'' is not limited to natural persons, but includes any type of organization, association or group such as other covered entities, health oversight agencies and advocacy groups.

Comment: A few commenters suggested deleting this provision in its entirety. One commenter indicated that the whistleblower and retaliation provisions could be inappropriately used against a hospital and that the whistleblower's ability to report numerous violations will result in a dangerous expansion of liability. Another commenter stated that covered entities could not take action against an employee who had violated the employer's privacy provisions if this employee files a complaint with the Secretary.

Several commenters suggested deleting ''in any manner'' and ''or opposing any act or practice made unlawful by this subpart'' in § 164.522(d)(4). The commenters indicated that, as proposed, the rule would make it difficult to enforce compliance within the workforce. One commenter stated that the proposed 164.522(d)(4) ''is extremely broad and may allow an employee to reveal protected health information to fellow employees, the media and others (e.g., an employee may show a medical record to a friend or relative before filing a complaint with the Department). This commenter further stated that covered entities will ''absolutely be prevented from prohibiting such conduct.'' One commenter suggested adding that a covered entity may take disciplinary action against any member of its work force or any business partner who uses or discloses individually identifiable health information in violation of this subpart in any manner other than through the processes set forth in the regulation.

Response: To respond to these comments, we make several changes to the proposed provision.

First, where the activity does not involve the filing of a complaint under § 160.306 of this part or participation in an investigation or proceeding initiated by the government under the rule, we delete the phrase ''in any manner'' and add a requirement that the individual's opposition to ''any act or practice'' made unlawful by this subpart be in good faith, and that the expression of that opposition must be reasonable. Second, we add a requirement that the individual's opposition to ''any act or practice'' made unlawful by this subpart must not involve a disclosure of protected health information that is in violation of this subpart. Thus, the employee who discloses protected health information to the media or friends is not protected. In providing interpretations of the retaliation provision, we will consider existing interpretations of similar provisions such as the guidance issued by EEOC in this regard.

Section 164.530(h)—Waiver of Rights

There are no comments directly about this section because it was not included in the proposed rule.

Section 164.530(i)—Policies and Procedures and § 164.530(j)—Documentation Requirements

Comments: Many of the comments to this provision addressed the costs and

complexity of the regulation as a whole, not the additional costs of documenting policies and procedures per se. Some did, either implicitly or explicitly, object to the need to develop and document policies and procedures as creating excessive administrative burden. Many of these commenters also asserted that there is a contradiction between the administrative burden of this provision and one of the statutory purposes of this section of the HIPAA to reduce costs through administrative simplification. Suggested alternatives were generally reliance on existing regulations and ethical standards, or on current business practices.

Response: A specific discussion of cost and burden is found in the Regulatory Impact Analysis of this final rule.

We do not believe there is a contradiction between the administrative costs of this provision and of the goal of administrative simplification. In the Administrative Simplification provisions of the HIPAA, Congress combined a mandate to facilitate the efficiencies and cost savings for the health care industry that the increasing use of electronic technology affords, with a mandate to improve privacy and confidentiality protections. Congress recognized, and we agree, that the benefits of electronic commerce can also cause increased vulnerability to inappropriate access and use of medical information, and so must be balanced with increased privacy protections. By including the mandate for privacy standards in section 264 of the HIPAA, Congress determined that existing regulations and ethical standards, and current business practices were insufficient to provide the necessary protections.

Congress mandated that the total benefits associated with administrative simplification must outweigh its costs, including the costs of implementing the privacy regulation. We are well within this mandate.

Comments: Several commenters suggested that the documentation requirements not be established as a standard under the regulation, because standards are subject to penalties. They recommend we delete the documentation standards and instead provide specific guidance and technical assistance. Several commenters objected to the suggestion in the NPRM that professional associations assist their members by developing appropriate policies for their membership. Several commentators representing professional associations believed this to be an onerous and costly burden for the associations, and suggested instead that we develop specific models which might require only minor modification. Some of these same associations were also concerned about liability issues in developing such guidelines. One commenter argued that sample forms, procedures, and policies should be provided as part of the Final Rule, so that practitioners would not be overburdened in meeting the demands of the regulations. They urged us to apply this provision only to larger entities.

Response: The purpose of requiring covered entities to develop policies and procedures for implementing this regulation is to ensure that important decisions affecting individuals' rights and privacy interests are made thoughtfully, not on an ad hoc basis. The purpose of requiring covered entities to maintain written documentation of these policies is to facilitate workforce training, and to facilitate creation of the required notice of information practices. We further believe that requiring written documentation of key decisions about privacy will enhance accountability, both within the covered entity and to the Department, for compliance with this regulation.

We do not include more specific guidance on the content of the required policies and procedures because of the vast difference in the size of covered entities and types of covered entities' businesses. We believe that covered entities should have the flexibility to design the policies and procedures best suited to their business and information practices. We do not exempt smaller entities, because the privacy of their patients is no less important than the privacy of individuals who seek care from large providers. Rather, to address this concern we ensure that the requirements of the rule are flexible so that smaller covered entities need not follow detailed rules that might be appropriate for larger entities with complex information systems.

We understand that smaller covered entities may require some assistance, and intend to provide such technical assistance after publication of this rule. We hope to work with professional associations and other groups that target classes of providers, plans and patients, in developing specialized material for these groups. Our discussions with several such organizations indicate their intent to work on various aspects of model documentation, including forms. Because the associations' comments regarding concerns about liability did not provide sufficient details, we cannot address them here.

Comment: Many commenters discussed the need for a recognition of scalability of the policies and procedures of an entity based on size, capabilities, and needs of the participants. It was noted that the actual language of the draft regulations under § 164.520 did not address scalability, and suggested that some scalability standard be formally incorporated into the regulatory language and not rely solely on the NPRM introductory commentary.

Response: In § 164.530(i)(1) of the final rule, we specify that we require covered entities to implement policies and procedures that take into account the size of the covered entity and the types of activities that relate to protected health information undertaken by the covered entity.

Comment: One commenter objected to our proposal to allow covered entities to make uses or disclosures not permitted by their current notice if a compelling reason exists to make the use or disclosure and the entity documents the reasons and changes its policies within 30 days of the use or disclosure. The commenter argued that the subjective language of the regulation might give entities the ability to engage in post hoc justifications for violations of their own information practices and policies. The commenter suggested that there should be an objective standard for reviewing the covered entity's reasons before allowing the covered entity to amend its policies.

Response: We eliminate this provision from the final rule. The final rule requires each covered entity to include in its notice of information practices a statement of all permitted uses under this rule, not just those in which the covered entity actually engages in at the time of that notice.

Comment: Some commenters expressed concern that the required retention period in the NPRM applied to the retention of medical records.

Response: The retention requirement of this regulation only applies to the documentation required by the rule, for example, keeping a record of accounting for disclosures or copies of policies and procedures. It does not apply to medical records.

Comments: Comments on the six year retention period were mixed. Some commenters endorsed the six-year retention period for maintaining documentation. One of the comments stated this retention period would assist physicians legally. Other commenters believed that the retention period would be an undue burden. One commenter noted that most State Board of Pharmacy regulations require

pharmacies to keep records for two years, so the six year retention period would triple document retention costs.

Response: We established the retention period at six years because this is the statute of limitations for the civil monetary penalties. This rule does not apply to all pharmacy records, but only to the documentation required by this rule.

Section 164.530(k)—Group Health Plans

There were no comments directly about this section because it was not included in the proposed rule.

Section 164.532—Transition Provisions

Comment: Commenters urged the Department to clarify whether the ''reach of the transition requirement'' is limited to a particular time frame, to the provider's activities in a particular job, or work for a particular employer. For example, one commenter questioned how long a nurse is a covered entity after she moves from a job reviewing files with protected health information to an administrative job that does not handle protected health information; or whether an occupational health nurse who used to transmit first reports of injury to her company's workers' compensation carrier last year but no longer does so this year because of a carrier change still is a covered entity.

Response: Because this comment addresses a question of enforcement, we will address it in the enforcement regulation.

Comment: Several commenters sought clarification as to the application of the privacy rule to research already begun prior to the effective date or compliance date of the final rule. These commenters argued that applying the privacy rule to research already begun prior the rule's effective date would substantially overburden IRBs and that the resulting research interruptions could harm participants and threaten the reliability and validity of conclusions based upon clinical trial data. The commenters recommended that the rule grandfather in any ongoing research that has been approved by and is under the supervision of an IRB.

Response: We generally agree with the concerns raised by commenters. In the final rule, we have provided that covered entities may rely upon consents, authorizations, or other express legal permissions obtained from an individual for a specific research project that includes the treatment of individuals to use or disclose protected health information the covered entity obtained before or after the applicable compliance date of this rule as long as certain requirements are met. These consents, authorizations, or other express legal permissions may specifically permit a use or disclosure of individually identifiable health information for purposes of the project or be a general consent of the individual to participate in the project. A covered entity may use or disclose protected health information it created or received before or after the applicable compliance date of this rule for purposes of the project provided that the covered entity complies with all limitations expressed in the consent, authorization, or permission.

In regard to research projects that include the treatment of individuals, such as clinical trials, covered entities engaged in these projects will have obtained at least an informed consent from the individual to participate in the project. In some cases, the researcher may also have obtained a consent, authorization, or other express legal permission to use or disclose individually identifiable health information in a specific manner. To avoid disrupting ongoing research and because the participants have already agreed to participate in the project (which expressly permits or implies the use or disclosure of their protected health information), we have grandfathered in these consents, authorizations, and other express legal permissions.

It is unlikely that a research project that includes the treatment of individuals could proceed under the Common Rule with a waiver of informed consent. However, to the extent such a waiver has been granted, we believe individuals participating in the project should be able to determine how their protected health information is used or disclosed. Therefore, we require researchers engaged in research projects that include the treatment of individuals who obtained an IRB waiver of informed consent under the Common Rule to obtain an authorization or a waiver of such authorization from an IRB or a privacy board under § 164.512(i) of this rule.

If a covered entity obtained a consent, authorization, or other express legal permission from the individual who is the subject of the research, it would be able to rely upon that consent, authorization, or permission, consistent with any limitations it expressed, to use or disclose the protected health information it created or received prior to or after the compliance date of this regulation. If a covered entity wishes to use or disclose protected health information but no such consent, authorization, or permission exists, it must obtain an authorization pursuant to § 164.508 or obtain a waiver of authorization under § 164.512(i). To the extent such a project is ongoing and the researchers are unable to locate the individuals whose protected health information they are using or disclosing, we believe the IRB or privacy board under the criteria set forth in § 164.512(i) will be able to take that circumstance into account when conducting its review. In most instances, we believe this type of research will be able to obtain a waiver of authorization and be able to continue uninterrupted.

Comment: Several comments raised questions about the application of the rule to individually identifiable information created prior to (1) the effective date of the rule, and (2) the compliance dates of the rule. One commenter suggested that the rule should apply only to information gathered after the effective date of the final rule. A drug manufacturer asked what would be the effect of the rule on research on records compiled before the effective date of the rule.

Response: We disagree with the commenter's suggestion. The requirements of this regulation apply to all protected health information held by a covered entity, regardless of when or how the covered entity obtained the information. Congress required us to adopted privacy standards that apply to individually identifiable health information. While it limited the compliance date for health plans, covered health care providers, and healthcare clearinghouses, it did not provide similar limiting language with regard to individually identifiable health information. Therefore, uses and disclosures of protected health information made by a covered entity after the compliance date of this regulation must meet the requirements of these rules. Uses or disclosures of individually identifiable health information made prior to the compliance date are not affected; covered entities will not be sanctioned under this rule based on past uses or disclosures that are inconsistent with this regulation.

Consistent with the definition of individually identifiable health information in HIPAA, of which protected health information is a subset, we do not distinguish between protected health information in research records and protected health information in other records. Thus, a covered entity's research records are subject to this regulation to the extent they contain protected health information.

Section 164.534—Effective Date and Compliance Date

Section 1175(b)(1)(A) of the Act requires all covered entities other than small health plans to comply with a standard or implementation specification ''not later than 24 months after the date on which an initial standard or implementation specification is adopted or established''; section 1175(b)(1)(B) provides that small health plans must comply not later than 36 months after that date. The proposed rule provided, at proposed § 164.524 (which was titled ''Effective date''), that a covered entity was required to be in compliance with the proposed subpart E not later than 24 months following the effective date of the rule, except that small health plans were required to be in compliance not later than 36 months following the effective date of the rule.

The final rules retain these dates in the text of Subpart E, but denominate them as ''compliance dates,'' to distinguish the statutory dates from the date on which the rules become effective. The effective date of the final rules is 60 days following publication in the **Federal Register.**

Meaning of Effective Date

Comment: A number of commenters expressed confusion about the difference between the effective date of the rule and the effective date on which compliance was required (the statutory compliance dates set out at section 1175(b)(1), summarized above).

Response: The Department agrees that the title of proposed § 164.524 was confusing. Similar comments were received on the Transactions Rule. Those comments were addressed by treating the ''effective date'' of the rule as the date on which adoption takes effect (the ''Effective Date'' heading at the beginning of the preamble), while the dates provided for by section 1175(b)(1) of the statute were denominated as ''compliance dates.'' These changes are reflected in the definition of ''compliance date'' in § 160.103 below (initially published as part of the Transactions Rule) and are also reflected at § 164.524 below. Section 164.524 below has also been reorganized to follow the organization of the analogous provisions of the Transactions Rule. The underlying policy, however, remains as proposed.

Extend the Compliance Date

Comment: Some commenters recommended that the compliance date be extended. A number of comments objected that the time frame for compliance with the proposed standards is unrealistically short. It was pointed out that providers and others would have to do the following, among other things, prior to the applicable compliance date: assess their current systems and departments, determine which state laws were preempted and which were not, update and reprogram computer systems, train workers, create and implement the required privacy policies and procedures, and create or update contracts with business partners. One comment also noted that the task of coming into compliance during the same time period with the other regulations being issued under HIPAA would further complicate the task. These comments generally supported an extension of the compliance dates by one or more years. Other comments supported extending the compliance dates on the ground that the complexity of the tasks involved in implementing the regulation would be a heavy financial burden for providers and others, and that they should be given more time to comply, in order to spread the associated capital and workforce costs over a longer period. It was also suggested that there be provision for granting extensions of the compliance date, based on some criteria, such as a good faith effort to comply or that the compliance dates be extended to two years following completion of a ''state-by-state preemption analysis'' by the Department.

Response: The Secretary acknowledges that covered entities will have to make changes to their policies and procedures during the period between the effective date of the rules below and the applicable compliance dates. The delayed compliance dates which the statute provides for constitute a recognition of the fact changes will be required and are intended to permit covered entities to manage and implement these changes in an orderly fashion. However, because the time frames for compliance with the initial standards are established by statute, the Secretary has no discretion to extend them: Compliance is statutorily required ''not later than'' the applicable compliance date. Nor do we believe that it would be advisable to accomplish this result by delaying the effective date of the final rules beyond 60 days. Since the Transactions Rule is now in effect, it is imperative to bring the privacy protections afforded by the rules below into effect as soon as possible. Retaining the delayed effective date of 60 days, as originally contemplated, will minimize the gap between transactions covered by those rules and not also afforded protection under the rules below.

Phase-in Requirements

Comment: Several comments suggested that the privacy standards be phased in gradually, to ease the manpower and cost burdens of compliance. A couple of equipment manufacturing groups suggested that updating of various types of equipment would be necessary for compliance purposes, and suggested a phased approach to this—for example, an initial phase consisting of preparation of policies, plans, and risk assessments, a second phase consisting of bringing new equipment into compliance, and a final phase consisting of bringing existing equipment into compliance.

Response: As noted in the preceding response, section 1175(b)(1) does not allow the Secretary discretion to change the time frame within which compliance must be achieved. Congress appears to have intended the phasing in of compliance to occur during the two-year compliance period, not thereafter.

Compliance Gap Vis-à-Vis State Laws and Small Health Plans

Comment: Several comments stated that, as drafted, the preemption provisions would be effective as of the rule's effective date (*i.e.,* 60 days following publication), even though covered entities would not be required to comply with the rules for at least another two years. According to these comments, the ''preempted'' state laws would not be in effect in the interim, so that the actual privacy protection would decrease during that period. A couple of comments also expressed concern about how the preemption provisions would work, given the one-year difference in applicable compliance dates for small health plans and other covered entities. A state medical society pointed out that this gap would also be very troublesome for providers who deal with both ''small health plans'' and other health plans. One comment asked what entities that decided to come into compliance early would have to do with respect to conflicting state laws and suggested that, since all parties ''need to know with confidence which laws govern at the moment, * * * [t]here should be uniform effective dates.''

Response: We agree that clarification is needed with respect to the applicability of state laws in the interim between the effective date and the compliance dates. What the comments summarized above appeared to assume is that the preemption provisions of section 1178 operate to broadly and generally invalidate any state law that comes within their ambit. We do not agree that this is the effect of section

1178. Rather, what section 1178 does—where it acts to preempt—is to preempt the state law in question with respect to the actions of covered entities to which the state law applies. Thus, if a provision of state law is preempted by section 1178, covered entities within that state to which the state law applies do not have to comply with it, and must instead comply with the contrary federal standard, requirement, or implementation specification. However, as compliance with the contrary federal standard, requirement, or implementation specification is not required until the applicable compliance date, we do not view the state law in question as meeting the test of being ''contrary.'' That is, since compliance with the federal standard, requirement, or implementation standard is not required prior to the applicable compliance date, it is possible for covered entities to comply with the state law in question. See § 160.202 (definition of ''contrary''). Thus, since the state law is not ''contrary'' to an applicable federal standard, requirement, or implementation specification in the period before which compliance is required, it is not preempted.

Several implications of this analysis should be spelled out. First, one conclusion that flows from this analysis is that preemption is specific to covered entities and does not represent a general invalidation of state law, as suggested by many commenters. Second, because preemption is covered entity-specific, preemption will occur at different times for small health plans than it will occur for all other covered entities. That is, the preemption of a given state law for a covered entity, such as a provider, that is covered by the 24-month compliance date of section 1175(b)(1)(A) will occur 12 months earlier than the preemption of the same state law for a small health plan that is covered by the 36-month compliance date of section 1175(b)(1)(B). Third, the preemption occurs only for covered entities; a state law that is preempted under section 1178(a)(1) would not be preempted for persons and entities to which it applies who are not covered entities. Thus, to the extent covered entities or non-covered entities follow the federal standards on a voluntary basis (*i.e.,* the covered entity prior to the applicable compliance date, the non-covered entity at any time), the state law in question will not be preempted for them.

Small Health Plans

Comment: Several comments, pointing to the ''Small Business'' discussion in the preamble to the proposed rules, applauded the decision to extend the compliance date to three years for small businesses. It was requested that the final rules clarify that the three year compliance date applies to small doctors offices and other small entities, as well as to small health plans.

Response: We recognize that our discussion in the preamble to the proposed rules may have suggested that more covered entities came within the 36 month compliance date than is in fact the case. Again, this is an area in which we are limited by statute. Under section 1175(b) of the Act, only small health plans have three years to come into compliance with the standards below. Thus, other ''small businesses'' that are covered entities must comply by the two-year compliance date.

Coordination With the Security Standard

Comment: Several comments suggested that the security standard be issued either with or after the privacy standards. It was argued that both sets of standards deal with protecting health information and will require extensive personnel training and revisions to business practices, so that coordinating them would make sense. An equipment manufacturers group also pointed out that it would be logical for covered entities and their business partners to know what privacy policies are required in purchasing security systems, and that ''the policies on privacy are implemented through the security standards rather than having already finalized security standards drive policy.''

Response: We agree with these comments, and are making every effort to coordinate the final security standards with the privacy standards below. The privacy standards below are being published ahead of the security standards, which is also responsive to the stated concerns.

Prospective Application

Comment: Several comments raised questions about the application of the rule to individually identifiable information created prior to (1) the effective date of the rule, and (2) the compliance dates of the rule. One provider group suggested that the rule should apply only to information gathered after the effective date of the final rule. A drug manufacturer asked what would be the effect of the rule on research on records compiled before the effective date of the rule.

Response: These comments are addressed in connection with the discussion of § 164.532 above.

Impact Analyses

Cost/Benefit Analysis

Comment: Many commenters made general statements to the effect that the cost estimates for implementing the provisions of the proposed regulation were incomplete or greatly understated.

Response: The proposal, including the cost analysis, is, in effect, a first draft. The purpose of the proposal was to solicit public comment and to use those comments to refine the final regulation. As a result of the public comment, the Department has significantly refined our initial cost estimates for implementing this regulation. The cost analysis below reflects a much more complete analysis of the major components of the regulation than was presented in the proposal.

Comment: Numerous commenters noted that significant areas of potential cost had not been estimated and that if they were estimated, they would greatly increase the total cost of the regulation. Potential cost areas identified by various respondents as omitted from the analyses include the minimum disclosure requirements; the requisite monitoring by covered entities of business partners with whom they share private health information; creation of de-identified information; internal complaint processes; sanctions and enforcement; the designation of a privacy official and creation of a privacy board; new requirements for research/optional disclosures; and future litigation costs.

Response: We noted in the proposed rule that we did not have data from which to estimate the costs of many provisions, and solicited comments providing such data. The final analysis below reflects the best estimate possible for these areas, based on the information available. The data and the underlying assumptions are explained in the cost analysis section below.

Comment: A number of comments suggested that the final regulation be delayed until more thorough analyses could be undertaken and completed. One commenter stated that the Department should refrain from implementing the regulation until a more realistic assessment of costs could be made and include local governments in the process. Similarly, a commenter requested that the Department assemble an outside panel of health industry experts, including systems analysts, legal counsel, and management consultants to develop stronger estimates.

Response: The Department has engaged in extensive research, data collection and fact-finding to improve

the quality of its economic analysis. This has included comments from and discussions with the kinds of experts one commenter suggested. The estimates represent a reasonable assessment of the policies proposed.

Comment: Several commenters indicated that the proposed regulation would impose significant new costs on providers' practices. Furthermore, they believe that it runs counter to the explicit statutory intent of HIPAA's Administrative Simplification provisions which require that ''any standard adopted * * * shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.''

Response: As the Department explained in the Transactions Rule, this provision applies to the administrative simplification regulations of HIPAA in the aggregate. The Transactions Rule is estimated to save the health care system $29.9 billion in nominal dollars over ten years. Other regulations published pursuant to the administrative simplification authority in HIPAA, including the privacy regulation, will result in costs, but these costs are within the statutory directive so long as they do not exceed the $29.9 billion in estimated savings. Furthermore, as explained in the Transactions Rule, and the preamble to this rule, assuring privacy is essential to sustaining many of the advances that computers will provide. If people do not have confidence that their medical privacy will be protected, they will be much less likely to allow their records to be used for any purpose or might even avoid obtaining necessary medical care.

Comment: Several commenters criticized the omission of aggregate, quantifiable benefit estimates in the proposed rule. Some respondents argued that the analysis in the proposed rule used ''de minimis'' cost estimates to argue only that benefits would certainly exceed such a low barrier. These commenters further characterized the benefits analysis in the Notice of Proposed Rulemaking as ''hand waving'' used to divert attention from the fact that no real cost-benefit comparison is presented. Another commenter stated that the benefit estimates rely heavily on anecdotal and unsubstantiated inferences. This respondent believes that the benefit estimates are based on postulated, but largely unsubstantiated causal linkages between increased privacy and earlier diagnosis and medical treatment.

Response: The benefits of privacy are diffused and intangible but real. Medical privacy is not a good people buy or sell in a market; therefore, it is very difficult to quantify. The benefits discussion in the proposal reflects this difficulty. The examples presented in the proposal were meant to be illustrative of the benefits based on a few areas of medicine where some relevant data was available. Unfortunately, no commenters provided either a better methodological approach or better data for assessing the overall benefits of privacy. Therefore, we believe the analysis in the proposal represents a valid illustration of the benefits of privacy, and we do not believe it is feasible to provide an overall dollar estimate of the benefits of privacy in the aggregate.

Comment: One commenter criticized the benefit analysis as being incomplete because it did not consider the potential cost of new treatments that might be engendered by increased confidence in medical privacy resulting from the regulation.

Response: There is no data or model to reliably assess such long-term behavioral and scientific changes, nor to determine what portion of the increasingly rapid evolution of new improved treatments might stem from improved privacy protections. Moreover, to be complete, such analysis would have to include the savings that might be realized from earlier detection and treatment. It is not possible at this time to project the magnitude or even the direction of the net effects of the response to privacy that the commenter suggests.

Scope of the Regulation

Comment: Numerous commenters noted the potential cost and burden of keeping track in medical records of information which had been transmitted electronically, which would be subject to the rule, as opposed to information that had only been maintained in paper form.

Response: This argument was found to have considerable merit and was one of the reasons that the Department concluded that the final regulation should apply to all medical records maintained by covered entities, including information that had never been transmitted electronically. The costs analysis below reflects the change in scope.

Notice Requirements

Comment: Several commenters expressed their belief that the administrative and cost burdens associated with the notice requirements were understated in the proposed rule. While some respondents took issue with the policy development cost estimates associated with the notice, more were focused on its projected implementation and production costs. For example, one respondent stated that determining ''first service'' would be an onerous task for many small practices, and that provider staff will now have to manually review each patient's chart or access a computer system to determine whether the patient has been seen since implementation of the rule.

Response: The policy in the final rule has been changed to make the privacy policy notice to patients less burdensome. Providers will be able to distribute the notice when a patient is seen and will not have to distribute it to a patient more than once, unless substantive changes are made in the notice. This change will significantly reduce the cost of distributing the privacy notices.

Comment: Some commenters also took issue with the methodology used to calculate the cost estimates for notices. These respondents believe that the survey data used in the proposed rule to estimate the costs (*i.e.,* ''encounters,'' ''patients,'' and ''episodes'' per year) are very different concepts that, when used together, render the purported total meaningless. Commenters further stated that they can verify the estimate of 543 million patients cited as being seen at least once every five years.

Response: In the course of receiving treatment, a patient may go to a number of medical organizations. For example, a person might see a doctor in a physician's office, be admitted to a hospital, and later go to a pharmacy for medication. Each time a person ''encounters'' a facility, a medical record may be started or additions made to an existing record. The concept in the proposal was to identify the number of record sets that a person might have for purposes of estimating notice and copying costs. For example, whether a person made one or ten visits in the course of a year to a specific doctor would, for our purposes, be one record set because in each visit the doctor would most likely be adding information to an existing medical record. The comments demonstrated that we had not explained the concept well. As explained below we modified the concept to more effectively measure the number of record sets that exist and explain it more clearly.

Comment: Several commenters criticized the lack of supporting evidence for the cost estimates of notice development and dissemination. Another opinion voiced in the comments is that the estimated cost for plans of $0.75 per insured person is so low that it may cover postage, but it

cannot include labor and capital usage costs.

Response: Based on comments and additional fact finding, the Department was able to gain a better understanding of how covered entities would develop policies and disseminate information. The cost analysis below explains more fully how we derived the final cost estimates for these areas.

Comment: A commenter noted that privacy policy costs assume that national associations will develop privacy policies for members but HHS analysis does not account for the cost to the national associations. A provider cost range of $300–$3,000 is without justification and seems low.

Response: The cost to the national associations was included in the proposal estimates, and it is included in the final analysis (see below).

Comment: A commenter states that the notice costs discussion mixes the terms ''patients'', ''encounters'' and ''episodes'' and 397 million encounter estimate is unclear.

Response: A clearer explanation of the concepts employed in this analysis is provided below.

Systems Compliance Costs

Comment: Numerous commenters questioned the methodology used to estimate the systems compliance cost and stated that the ensuing cost estimates were grossly understated. Some stated that the regulation will impose significant information technology costs to comply with requirement to account for disclosures, additional costs for hiring new personnel to develop privacy policies, and higher costs for training personnel.

Response: Significant comments were received regarding the cost of systems compliance. In response, the Department retained the assistance of consultants with extensive expertise in health care information technology. We have relied on their work to revise our estimates, as described below. The analysis does not include ''systems compliance'' as a cost item, per se. Rather, in the final analysis we organized estimates around the major policy provisions so the public could more clearly see the costs associated with them. To the extent that the policy might require systems changes (and a number of them do), we have incorporated those costs in the provision's estimate.

Comment: Items explicitly identified by commenters as significantly adding to systems compliance costs include tracking disclosures of protected health information and patient authorizations; restricting access to the data; accommodating minimum disclosure provisions; installing notices and disclaimers; creating de-identified data; tracking uses of protected health information by business partners; tracking amendments and corrections; increased systems capacity; and annual systems maintenance. The commenters noted that some of the aforementioned items are acknowledged in the proposed rule as future costs to covered entities, but several others are singularly ignored.

Response: The Department recognizes the validity of much of this criticism. Unfortunately, other than general criticism, commenters provided no specific data or methodological information which might be used to improve the estimates. Therefore, the Department retained consultants with extensive expertise in these areas to assess the proposed regulation, which helped the Department refine its policies and cost estimates.

In addition, it is important to note that the other HIPAA administrative simplification regulations will require systems changes. As explained generally in the cost analysis for the electronic Transactions rule, it is assumed that providers and vendors will undertake systems changes for these regulations collectively, thereby minimizing the cost of changes.

Inspection and Copying

Comment: Numerous commenters disagreed with the cost estimates in the NPRM for inspection and copying of patient records, believing that they were too low.

Response: The Department has investigated the potential costs through a careful reading of the comments and subsequent factfinding discussions with a variety of providers. We believe the estimates, explained more fully below, represent a reasonable estimate in the aggregate. It is important to note, however, that this analysis is not measuring the cost of all inspection and copying because a considerable amount of this already occurs. The Department is only measuring the incremental increase likely to occur as a result of this regulation.

Comment: One commenter speculates that, even at a minimum charge of $.50/page, (and not including search and retrieval charges), costs could run as high as $450 million annually.

Response: The $0.50 per page in the proposal represent an average of several data sources. Subsequently, an industry commenter, which provided extensive medical records copying, stated that this was a reasonable average cost. Hence, we retained the number for the final estimate.

Comment: One respondent states that, since the proposed rules give patients the right to inspect and copy their medical records regardless of storage medium, HHS must make a distinction in its cost estimates between records stored electronically and those which must be accessed by manual means, since these costs will differ.

Response: The cost estimates made for regulations are not intended to provide such refined gradations; rather, they are intended to show the overall costs for the regulation as a whole and its major components. For inspections and copying (and virtually all other areas for which estimates are made) estimates are based on averages; particular providers may experience greater or lesser costs than the average cost used in this analysis.

Comment: Several commenters noted that the Department did not appear to include the cost of establishing storage systems, retrieval fees and the cost of searching for records, and that these costs, if included, would significantly increase the Department's estimate.

Response: Currently, providers keep and maintain medical records and often provide copies to other providers and patients. Therefore, much of the cost of maintaining records already exists. Indeed, based on public comments, the Department has concluded that there will be relatively few additional copies requested as the result of this regulation (see below). We have measured and attributed to this regulation the incremental cost, which is the standard for conducting this kind of analysis.

Comment: A federal agency expressed concern over the proposal to allow covered entities to charge a fee for copying personal health information based on reasonable costs. The agency requests personal health information from many covered entities and pays a fee that it establishes. Allowing covered entities to establish the fee, the agency fears, may cost them significantly more than the current amounts they pay and as a result, could adversely affect their program.

Response: The proposal and the final rule establish the right to access and copy records only for individuals, not other entities; the ''reasonable fee'' is only applicable to the individual's request. The Department's expectation is that other existing practices regarding fees, if any, for the exchange of records not requested by an individual will not be affected by this rule.

Appending Records (Amendment and Correction)

Comment: The proposed rule estimated the cost of amending and correcting patients' records at $75 per instance and $260 million per year for small entities. At least one commenter stated that such requests will rise significantly upon implementation of the regulations and increase in direct proportion to the number of patients served. Another commenter described the more subtle costs associated with record amendment and correction, which would include a case-by-case clinical determination by providers on whether to grant such requests, forwarding the ensuing record changes to business partners, and issuing written statements to patients on the reasons for denials, including a recourse for complaints.

Response: The comments were considered in revising the proposal, and the decision was made to clarify in the final regulation that providers must only append the record (the policy is explained further in the preamble and the regulation text). The provider is now only required to note in the medical record any comments from the patient; they may, but are not required to, correct any errors. This change in policy significantly reduces the cost from the initial proposal estimate.

Comment: Several commenters criticized the proposed rule's lack of justification for assumptions regarding the percentage of patients who request inspection and copying, who also request amendment and correction. Another commenter pointed out that the cost estimate for amendment and correction is dependent on a base assumption that only 1.5 percent of patients will request inspection of their records. As such, if this estimate were too low by just one percentage point, then the estimates for inspection and copying plus the costs for amendment and correction could rise by 67 percent.

Response: Based on information and data received in the public comments, the estimate for the number of people requesting inspection and copying has been revised. No commenter provided specific information on the number of amended record requests that might result, but the Department subsequently engaged in fact-finding and made appropriate adjustments in its estimates. The revisions are explained further below.

Consent and Authorizations

Comment: One respondent indicated that the development, collection, and data entry of all the authorizations will create a new transaction type for employers, health plans, and providers, and result in duplicated efforts among them. This commenter estimates that the costs of mailing, re-mailing, answering inquiries, making outbound calls and performing data entry in newly created authorization computer systems could result in expenses of close to $2.0 billion nationally. Another commenter indicated that authorization costs will be at least double the notice dissemination costs due to the cost of both outbound and return postage.

Response: Public commenters and subsequent factfinding clearly indicate that most providers with patient contact already obtain authorizations for release of records, so for them there is virtually no new cost. Further, this comment does not reflect the actual regulatory requirement. For example, there is no need to engage in mailing and re-mailing of forms, and we do not foresee any reason why there should be any significant calls involved.

Comment: A commenter criticized the percentage (1%) that we used to calculate the number of health care encounters expected to result in requests to withhold the release of protected information. This respondent postulates that even if one in six patients who encounter the U.S. health care system opt to restrict access to their records, the total expected national cost per year could rise to $900 million.

Response: The final regulation requirements regarding the release of protected health information has been substantially changed, thereby greatly reducing the potential cost burden. A fuller explanation of the cost is provided below in the regulatory impact analysis.

Comment: An additional issue raised by commenters was the added cost of seeking authorizations for health promotion and disease management activities, health care operations that traditionally did not require such action.

Response: In the final regulation, a covered entity can use medical information collected for treatment or operations for its own health promotion and disease management efforts without obtaining additional authorization. Therefore, there is no additional cost incurred.

Business Associates

Comment: A number of commenters were concerned about the cost of monitoring business partners. Specifically, one commenter stated that the provisions of the proposed regulation pertaining to business partners would likely force the discontinuation of outsourcing for some functions, thereby driving up the administrative cost of health care.

Response: The final regulation clarifies the obligations of the business associates in assuring privacy. As explained in the preamble, business associates must take reasonable steps to assure confidentiality of health records they may have, and the covered entity must take appropriate action if they become aware of a violation of the agreement they have with the business associate. This does not represent an unreasonable burden; indeed, the provider is required to take the same kind of precautions and provide the same kind of oversight that they would in many other kinds of contractual relationships to assure they obtain the quality and level of performance that they would expect from a business associate.

Comment: HHS failed to consider enforcement costs associated with monitoring partners and litigation costs arising from covered entities seeking restitution from business partners whose behavior puts the covered entity at risk for noncompliance.

Response: The Department acknowledged in the proposal that it was not estimating the cost of compliance with the business associates provision because of inadequate information. It requested information on this issue, but no specific information was provided in the comments. However, based on revisions in the final policy and subsequent factfinding, the Department has provided an estimate for this requirement, as explained below.

Training

Comment: Many of the commenters believe that the Department used unrealistic assumptions in the development of the estimated cost of the training provisions and they provided their own estimates.

Response: The commenters' estimates varied widely, and could not be used by the Department in revising its analysis because there was inadequate explanation of how the estimates were made.

Comment: Several commenters argued that if even an hour of time of each of the entity's employees is spent on training instead of ''work'' and they are paid the minimum wage, an entity would incur $100 of cost for training no more than 20 employees. The commenters noted that the provision of health care services is a labor-intensive enterprise, and many covered entities have thousands of employees, most of whom make well in excess of minimum

wage. They questioned whether the estimates include time taken from the employee's actual duties (opportunity cost) and the cost of a trainer and materials.

Response: As explained in more detail below, the Department made extensive revisions in its training estimate, including the number of workers in the health care sector, the cost of workers in training based on average industry wages, and training costs (instructors and materials). The revised estimate is a more complete and accurate estimate of the costs likely to be borne as a result of the final regulation.

Comment: One commenter estimated that simply training an employee could have a burdensome impact on his company. He argued, for example, a 10-hour annual requirement takes 0.5% of an employee's time if they work a 2000-hour year, but factoring in sick and vacation leave, the effects of industry turnover could significantly increase the effect.

Response: In the analysis below, the Department has factored in turnover rates, employment growth and greater utilization based on data obtained from broad-based surveys and a public comment.

Comment: Some commenters felt that the regulatory training provisions are overly burdensome. Specific concerns centered around the requirement to train all individuals who may come in contact with protected health information and the requirement to have such individuals sign a new certifying statement at least every three years. Some commenters felt that the content of the training program should be left to the discretion of the covered entity.

Response: Changes and clarifications in the training requirements are made in the final regulation, explained below. For example, the certification requirement has been eliminated. As in the NPRM, the content of the training program is left to the discretion of the covered entity. These changes are expected to lessen the training burden and are reflected in the final cost estimates.

Compliance and Enforcement

Comment: A Member of Congress and a number of privacy and consumer groups expressed their concern with whether the Office for Civil Rights (OCR) in HHS has adequate funding to carry out the major responsibility of enforcing the complaint process established by this rule. The Member stated that ''[d]ue to the limited enforcement ability allowed for in this rule by HIPAA, it is essential that OCR have the capacity to enforce the regulations. Now is the time for The Secretary to begin building the necessary infrastructure to enforce the regulation effectively.''

Response: The Secretary agrees with the commenters and is committed to an effective enforcement program. We will work with Congress to ensure that the Department has the necessary funds to secure voluntary compliance through education and technical assistance, to investigate complaints and conduct compliance reviews, to provide states with exception determinations and to use civil and criminal penalties when necessary.

Economic Effect on Small Entities

Comment: Many commenters stated that the cost estimates on the effect of the proposed regulation on small businesses were understated or incomplete.

Response: The Department conducted a thorough review of potential data sources that would improve the quality of the analysis of the effects on small business. The final regulatory flexibility analysis below is based on the best data available (much of it from the Small Business Administration) and represents a reliable estimate for the effects on small entities in various segments of the health care industry. It is important to note that the estimates are for small business segments in the aggregate; the cost to individual firms will vary, perhaps considerably, based on its particular circumstances.

Comment: The cost of implementing privacy regulations, when added to the cost of other required HIPAA regulations, could increase overhead significantly. As shown in the 1993 Workgroup on Electronic Data Interchange (WEDI) Report, providers will bear the larger share of implementation costs and will save less than payors.

Response: The regulatory flexibility analysis below shows generally the marginal effect of the privacy regulation on small entities. Collectively, the HIPAA administrative standards will save money in the health care system. As important, given the rapid expansion of electronic commerce, it is probable that small entities would need to comply with standards for electronic commerce in order to complete effectively, even if the standards were voluntary. The establishment of uniform standards through regulation help small entities because they will not have to invest in multiple systems, which is what they would confront if the system remained voluntary.

Comment: One respondent believed that the initial and ongoing costs for small provider offices could be as much as 11 times higher than the estimates provided in the proposed rule. Other commenters stated that the estimates for small entities are ''absurdly low''.

Response: Although there were a number of commenters highly critical of the small business analysis, none provided alternative estimates or even provided a rationale for their statements. Many appeared to assume that all costs associated with medical record confidentiality should be estimated. This represents a misunderstanding of the purpose of the analysis: to estimate the incremental effects of this regulation, *i.e.,* the new costs (and savings) that will result from changes required by the regulation. The Department has made substantial changes in the final small entities analysis (below), reflecting policy changes in the final rule and additional information and data collected by the Department since the issuance of the proposal last fall. We believe that these estimates reasonably reflect the costs that various types of small entities will experience in general, though the actual costs of particular providers might vary considerably based on their current practices and technology.

Comment: A respondent expressed the belief that small providers would bear a disproportionate share of the regulation's administrative burden because of the likelihood of larger companies incurring fewer marginal costs due to greater in-house resources to aid in the legal and technical analysis of the proposed rule.

Response: As explained below, the Department does not agree with the assertion that small entities will be disproportionately affected. Based on discussions with a number of groups, the Department expects many professional and trade associations to provide their members with analysis of the regulation, including model policies, statements and basic training materials. This will minimize the cost for most small entities. Providers that use protected health information for voluntary practices, such as marketing or research, are more likely to need specific legal and technical assistance, but these are likely to be larger providers.

Comment: Several commenters took issue with the ''top-down'' approach that we used to estimate costs for small businesses, believing that this methodology provided only a single point estimate, gave no indication of the variation around the estimate, and was subject to numerous methodological errors since the entities to which the numerator pertained may not have been

the same as the denominator. These respondents further recommended that we prepare a ''bottom-up'' analysis using case studies and/or a survey of providers to refine the estimates.

Response: The purpose of the regulatory flexibility analysis is to provide a better insight into the relative burden of small businesses compared to larger firms in complying with a regulation. There may be considerable variance around average costs within particular industry sectors, even among small businesses within them. The estimates are based on the best data available, including information from the Small Business Administration, the Census Bureau, and public comments.

Comment: A commenter stated that the proposal's cost estimate does not account for additional administrative costs imposed on physicians, such as requirements to rewrite contracts with business partners.

Response: Such costs are included in the analysis below.

Comment: Numerous public comments were directed specifically at the systems compliance cost estimates for small businesses. One respondent maintained that the initial upgrade cost alone would range from $50 thousand to more than $1 million per covered entity.

Response: The cost estimates for systems compliance varied enormously; unfortunately, none of the commenters provided documentation of how they made their estimates, preventing us from comparing their data and assumptions to the Department's. Because of concern about the costs in this area, however, the Department retained an outside consultant to provide greater expertise and analysis. The product of this effort has been incorporated in the analysis below.

Comment: One commenter stated that just the development and documentation of new health information policies and procedures (which would require an analysis of the federal regulations and state law privacy provisions), would cost far more than the $396 cited in the Notice of Proposed Rulemaking as the average start-up cost for small businesses.

Response: As explained below in the cost analysis, the Department anticipates that most of the policies and procedures that will be required under the final rule will be largely standardized, particularly for small businesses. Thus, much of the work and cost can be done by trade associations and professional groups, thereby minimizing the costs and allowing it to be spread over a large membership base.

Comment: A number of comments criticized the initial estimates for notices, inspection and copying, amendments and correction, and training as they relate to small businesses.

Response: The Department has made substantial revisions in its estimates for all of these areas which is explained below in the regulatory flexibility analysis.

Comment: One commenter noted that there appeared to be a discrepancy in the number of small entities cited. There is no explanation for the difference and no explanation for difference between ''establishments'' and ''entities.''

Response: There are discrepancies among the data bases on the number of ''establishments'' and ''entities'' or ''firms''. The problem arises because most surveys count (or survey) establishments, which are physical sites. A single firm or entity may have many establishments. Moreover, although an establishment may have only a few employees, the firm may have a large number of workers (the total of all its various establishments) and therefore not be a small entity.

As discussed below, there is some discrepancy between the aggregate numbers we use for the regulatory impact analysis (RIA) and the regulatory flexibility analysis (RFA). We concluded that for purposes of the RFA, which is intended to measure the effects on small entities, we would use Small Business Administration data, which defines entities based on revenues rather than physical establishments to count the number of small entities in various SIC. This provides a more accurate estimate of small entities affected. For the RIA, which is measuring total effects, we believe the establishment based surveys provide a more reliable count.

Comment: Because small businesses must notify patients of their privacy policies on patients' first visit after the effective date of the regulation, several commenters argued that staff would have to search records either manually or by computer on a daily basis to determine if patients had been seen since the regulation was implemented.

Response: Under the final regulation, all covered entities will have to provide patients copies of their privacy policy at the first visit after the effective date of the regulation. The Department does not view this as burdensome. We expect that providers will simply place a note or marker at the beginning of a file (electronic or paper) when a patient is given the notice. This is neither time-consuming nor expensive, and it will not require constant searches of records.

Comment: A commenter stated that the definitions of small business, small entity, and a small health plan are inconsistent because the NPRM includes firms with annual receipts of $5 million or less and non-profits.

Response: The Small Business Administration, whose definitions we use for this analysis, includes firms with $5 million or less in receipts and all non-profits as ''small businesses.'' We recognize that some health plans, though very large in terms of receipts (and insured lives), nonetheless would be considered ''small businesses'' under this definition because they are non-profits. In the final regulatory flexibility analysis, we generally have maintained the Small Business Administration definitions because it is the accepted standard for these analyses. However, we have added several categories, such as IRBs and employer sponsored group health plans, which are not small entities, per se, but will be effected by the final rule and we were able to identify costs imposed by the regulation on them.

Comment: The same commenter wanted clarification that all non-profit organizations are small entities and that the extended effective date for compliance applies to them.

Response: For purposes of the regulatory flexibility analysis, the Department is utilizing the Small Business Administration guidelines. However, under HIPAA the Secretary may extend the effective compliance date from 24 months to 36 months for ''small health plans''. The Secretary is given the explicit discretion of defining the term for purposes of compliance with the regulation. For compliance purposes, the Secretary has decided to define ''small health plans'' as those with receipts of $5 million or less, regardless of their tax status. As noted above, some non-profit plans are large in terms of revenues (*i.e.,* their revenues exceed $5 million annually). The Department determined that such plans do not need extra time for compliance.

Comment: Several commenters requested that ''small providers'' [undefined] be permitted to take 36 months to come into compliance with the final regulation, just as small health plans will be permitted to do so.

Response: Congress specified small health plans, but not small providers, as needing extra time to comply. The majority of providers affected by the regulation are ''small'', based on the SBA definitions; in other words, granting the delay would be tantamount to make the effective date three years rather than two. In making policy decisions for the final regulation, extensive consideration was given to minimizing the cost and administrative burden associated with implementing

the rule. The Department believes that the requirements of the final rule will not be difficult to fulfill, and therefore, it has maintained the two year effective date.

External Studies

Comment: One commenter submitted a detailed analysis of privacy legislation that was pending and concluded that they might cost over $40 billion.

Response: The study did not analyze the policies in the proposal, and therefore, the estimates do not reflect the costs that would have been imposed by the proposed regulation. In fact, the analysis was prepared before the Administration's proposed privacy regulation was even published. As a result, the analysis is of limited relevance to the regulation actually proposed.

The following are examples of assumptions and costs in the analysis that do not match privacy policies or requirements stated in the proposed rule.

1. *Authorizations:* The study assumed rules requiring new authorizations from current subscribers to use their data for treatment, payment of claims, or other health plan operations. The proposed rule would have prohibited providers or plans from obtaining patient authorization to use data for treatment, payment or health care operations, and the final rule makes obtaining consent for these purposes voluntary for all health plans and for providers that do not have direct treatment relationships with individuals.

2. *Disclosure History:* The study assumes that providers, health plans, and clearinghouses would have to track all disclosures of health information. Under the NPRM and the final rule, plans, providers and clearinghouses are only required to account for disclosures that are not for treatment, payment, and health care operations, a small minority of all disclosures.

3. *Inspection, Copying, and Amendment:* The study assumed requirements to allow patients and their subscribers to inspect, copy, and amend all information that includes their name, social security number or other identifying feature (*e.g.* customer service calls, internal memorandum, claim runs). However, the study assumed broader access than provided in the rule, which requires access only to information in records used to make decisions about individuals, not all records with identifiable information.

4. *Infrastructure development:* The study attributed significant costs to infrastructure implementation of (computer systems, training, and other compliance costs). As explained below, the compliance requirements are much less extensive than assumed in this study. For example, many providers and plans will not be required to modify their privacy systems but will only be required to document their practices and notify patients of these practices, and others will be able to purchase low-cost, off-the-shelf software that will facilitate the new requirements. The final regulation will not require massive capital expenditures; we assumed, based on our consultants' work, that providers will rely on low-cost incremental adjustments initially, and as their technology becomes outdated, they will replace it with new systems that incorporate the HIPAA standard requirements.

Although many of the policy assumptions in the study are fundamentally different than those in the proposed or final regulation, the study did provide some assistance to the Department in preparing its final analysis. The Department compared data, methodologies and model assumptions, which helped us think more critically about our own analysis and enhanced the quality of our final work.

Comment: One commenter submitted a detailed analysis of the NPRM Regulatory Impact Analysis and concluded that it might cost over $64 billion over 5 years. This analysis provided an interesting framework for analyzing the provision for the rule. More precisely, the analysis generally attempted to identify the number of entities would be required to comply with each of the significant provision of the proposed rule, then estimated the numbers of hours required to comply per entity, and finally, estimated an hourly wage.

Response: HHS adopted this general structure for the final RIA because it provided a better framework for analysis than what the Department had done in the NPRM. However, HHS did not agree with many of the specific assumptions used by in this analysis, for several reasons. First, in some instances the assumptions were no longer relevant because the requirements of the NPRM were altered in the final rule. For other assumptions, HHS found more appropriate data sources for the number of covered entities, wages rates and trend rates or other factors affecting costs. In addition, HHS believes that in a few instances, this analysis over-estimated what is required of covered entities to comply. Based on public comments and its own factfinding, the Department believes many of its assumptions used in the final analysis more accurately reflect what is likely to be the real cost of the regulation.

IV. Final Regulatory Impact Analysis

5 U.S.C. 804(2) (as added by section 251 of Pub. L. 104–21), specifies that a ''major rule'' is any rule that the Office of Management and Budget finds is likely to result in:

- An annual effect on the economy of $100 million or more;
- A major increase in costs or prices for consumers, individual industries, federal, state, or local government agencies, or geographic regions; or
- Significant adverse effects in competition, employment, investment productivity, innovation, or on the ability of United States based enterprises to compete with foreign-based enterprises in domestic and export markets. The impact of this final rule will be over $1 billion in the first year of implementation. Therefore, this rule is a major rule as defined in 5 U.S.C. 804(2).

Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects; distributive impacts; and equity). According to Executive Order 12866, a regulatory action is ''significant'' if it meets any one of a number of specified conditions, including having an annual effect on the economy of $100 million or more adversely affecting in a material way a sector of the economy, competition, or jobs, or if it raises novel legal or policy issues. The purpose of the regulatory impact analysis is to assist decision-makers in understanding the potential ramifications of a regulation as it is being developed. The analysis is also intended to assist the public in understanding the general economic ramifications of a regulation, both in the aggregate as well as the major policy areas of a regulation and how they are likely to affect the major industries or sectors of the economy covered by it.

In accordance with the Small Business Regulatory Enforcement and Fairness Act (Pub. L. 104–121), the Administrator of the Office of Information and Regulatory Affairs of the Office of Management and Budget (OMB) has determined that this rule is a major rule for the purpose of congressional review.

The proposal for the privacy regulation included a preliminary regulatory impact analysis (RIA) which estimated the cost of the rule at $3.8 billion over five years. The preliminary

analysis also noted that a number of significant areas were not included in the estimate due to inadequate information. The proposal solicited public comment on these and all other aspects of the analysis. In this preamble, the Department has summarized the public comments pertinent to the cost analysis and its response to them. However, because of the extensive policy changes incorporated in the final regulation, additional data collected from the public comments and the Department's fact-finding, and changes in the methodology underlying the estimates, the Department is setting forth in this section a more complete explanation of its revised estimates and how they were obtained. This will facilitate a better understanding by the public of how the estimates were developed and provide more insight into how the Department believes the regulation will ultimately affect the health care sector.

The impact analysis measures the effect of the regulation on current practices. In the case of privacy, as discussed in the preamble, there already exists considerable, though quite varied, efforts to protect the confidentiality of medical information. The RIA is measuring the change in these current practices and the cost of new and additional responsibilities that are required to conform to the new regulation.

To achieve a reasonable level of privacy protection, the Department defined three objectives for the final rule: (1) To establish national baseline standards, implementation specifications, and requirements for health information privacy protection, (2) to protect the privacy of individually identifiable health information maintained or transmitted by covered entities, and (3) to protect the privacy of all individually identifiable health information within covered entities, regardless of its form.

Establishing minimum standards, implementation specifications, and requirements for health information privacy protection creates a level baseline of privacy protection for patients across states. The Health Privacy Project's report, *The State of Health Privacy: An Uneven Terrain* [33] makes it clear that under the current system of state laws, privacy protection is extremely variable. The Department's statutory authority under HIPAA which allows the privacy regulation to preempt any state law if such law is contrary to and not more stringent than privacy protection pursuant to this regulation. This sets a floor, but permits a state to create laws that are more protective of privacy. We discuss preemption in greater detail in other parts of the preamble.

The second objective is to establish a uniform base of privacy protection for individually identifiable health information maintained or transmitted by covered entities. HIPAA restricts the type of entities covered by the rule to three broad categories: health care providers that transmit health information in HIPAA standard transactions, health plans, and health care clearinghouses. However, there are similar public and private entities that are not within the Department's authority to regulate under HIPAA. For example, life insurance companies are not covered by this rule but may have access to a large amount of individually identifiable health information.

The third objective is to protect the privacy of all individually identifiable health information held by covered entities, including their business associates. Health information is currently stored and transmitted in multiple forms, including electronic, paper, and oral forms. To provide consistent protection to information, and to avoid requiring covered entities from distinguishing between health information that has been transmitted or maintained electronically and that which has not, this rule covers all individually identifiable health information in any form maintained or transmitted by a covered entity.

For purposes of this cost analysis, the Department has assumed all health care providers will be affected by the rule. This results in an overestimation of costs because there are providers that do not engage in any HIPAA standard transactions, and therefore, are not affected. The Department could not obtain any reliable data on the number of such providers, but the available data suggest that there are very few such entities, and given the expected increase in all forms of electronic health care in the coming decade, the number of paper-only providers is likely to decrease.

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

Congress has recognized that privacy standards, implementation specifications and requirements must accompany the electronic data interchange standards, implementation specifications and requirements because the increased ease of transmitting and sharing individually identifiable health information will result in an increase in concern regarding privacy and confidentiality of such information. The bulk of the first Administrative Simplification section that was debated on the floor of the Senate in 1994 (as part of the Health Security Act) was made up of privacy provisions. The requirement for the issuance of concomitant privacy measures remained a part of the HIPAA bill passed by the House of Representatives in 1996, but the requirement for privacy measures was removed in conference. Instead, Congress added section 264 to Title II of HIPAA, which directs the Secretary to develop and submit to Congress recommendations addressing at least the following:

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

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

(3) The uses and disclosures of such information that should be authorized or required. The Secretary's Recommendations were submitted to Congress on September 11, 1997, and are summarized below. Section 264(c)(1) of HIPAA provides that: If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by (August 21, 1999), the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than (February 21, 2000). Such regulations shall address at least the subjects described in subsection (regarding recommendations).

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

Title II of the Health Insurance Portability and Accountability Act (HIPAA) also provides a statutory framework for the promulgation of other administrative simplification regulations. On August 17, 2000, the Transactions Rule was published. Proposals for health care provider identifier (May 1998), employer identifier (June 1998), and security and electronic signature standards (August 1998) have also been published. These

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

regulations are expected to be made final in the foreseeable future.

HIPAA states that, ''any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.'' (Section 1172 (b)). This provision refers to the administrative simplification regulations in their totality, including this rule regarding privacy standards. The savings and costs generated by the various standards should result in a net savings to the health care system. The Transactions Rule shows a net savings of $29.9 billion over ten years (2002–2011), or a net present value savings of $19 billion. This estimate does not include the growth in ''e-health'' and ''e-commerce'' that may be spurred by the adoption of uniform codes and standards.

This final Privacy Rule is estimated to produce net costs of $18.0 billion, with net present value costs of $11.8 billion (2003 dollars) over ten years (2003–2012). This estimate is based on some costs already having been incurred due to the requirements of the Transactions Rule, which included an estimate of a net savings to the health care system of $29.9 billion over ten years (2002 dollars) and a net present value of $19.1 billion. The Department expects that the savings and costs generated by all administrative simplification standards should result in a net savings to the health care system.

B. Summary of Costs and Benefits

Measuring both the economic costs and benefits of health information privacy is difficult. Traditionally, privacy has been addressed by state laws, contracts, and professional practices and guidelines. Moreover, these practices have been evolving as computers have dramatically increased the potential use of medical data; the scope and form of health information is likely to be very different ten years from now than it is today. This final regulation is both altering current health information privacy practice and shaping its evolution as electronic uses expand.

To estimate costs, the Department used information from published studies, trade groups and associations, public comments to the proposed regulation, and fact-finding by staff. The analysis focused on the major policy areas in the regulation that would result in significant costs. Given the vast array of institutions affected by this regulation and the considerable variation in practices, the Department sought to identify the ''typical'' current practice for each of the major policy areas and estimate the cost of change resulting from the regulation. Because of the paucity of data and incomplete information on current practices, the Department has consistently made conservative assumptions (that is, given uncertainty, we have made assumptions that, if incorrect, are more likely to overstate rather than understate the true cost).

Benefits are difficult to measure because people conceive of privacy primarily as a right, not as a commodity. Furthermore, a wide gap appears to exist between what people perceive to be the level of privacy afforded health information about them and what actually occurs with the use of such information today. Arguably, the ''cost'' of the privacy regulation is the amount necessary to bring health information privacy to these perceived levels.

The benefits of enhanced privacy protections for individually identifiable health information are significant, even though they are hard to quantify. The Department solicited comments on this issue, but no commenters offered a better alternative. Therefore, the Department is essentially reiterating the analysis it offered in the proposed Privacy Rule. The illustrative examples set forth below, using existing data on mental health, cancer screening, and HIV/AIDS patients, suggest the level of economic and health benefits that might accrue to individuals and society. Moreover, the benefits of improved privacy protection are likely to increase in the future as patients gain trust in health care practitioners' ability to maintain the confidentiality of their health information.

The estimated cost of compliance with the final rule is $17.6 billion over the ten year period, 2003–2012.[34] This includes the cost of all the major requirements for the rule, including costs to federal, state and local governments. The net present value of the final rule, applying a 11.2 percent discount rate[35], is $11.8 billion.[36]

The first year estimate is $3.2 billion (this includes expenditures that may be incurred before the effective date in 2003). This represents about 0.23 percent of projected national health expenditures for 2003.[37] By 2008, seven years after the rule's effective date, the rule is estimated to cost 0.07 percent of projected national health expenditures.

The largest cost items are the requirement to have a privacy official, $5.9 billion over ten years, and the requirement that disclosures of protected health information only involve the minimum amount necessary, $5.8 billion over ten years (see Table 1). These costs reflect the change that affected organizations will have to undertake to implement and maintain compliance with the requirements of the rule and achieve enhanced privacy of protected health information.

[34] The proposed privacy rule provided an estimate for a five-year period. However, the Transactions Rule provided a cost estimate for a ten year period. The decision was made to provide the final privacy estimates in a ten year period so that it would be possible to compare the costs and benefits of the two regulations.

[35] This based on a seven percent real discount rate, explained in OMB Circular A–94, and a projected 4.2 percent inflation rate projected over the ten-year period covered by this analysis.

[36] The regulatory impact analysis in the Transactions Rule showed a net savings of $29.9 billion (net present value of $19.1 billion in 2002 dollars). The cost estimates included all electronic systems changes that would be necessitated by the HIPAA administrative standards (*e.g.,* security, safeguards, and electronic signatures; eligibility for a health plan; and remittance advice and payment claim status), except privacy. At the time the Transactions Rule was developed, the industry provided estimates for the systems changes in the aggregate. The industry argued that affected parties would seek to make all electronic changes in one effort because that approach would be the most cost-efficient. The Department agreed, and therefore, it ''bundled'' all the system change cost in the Transactions Rule estimate. Privacy was not included because at the time the Department had not made a decision to develop a privacy rule. As the Department develops other HIPAA administrative simplification standards, there may be additional costs and savings due to the non-electronic components of those regulations, and they will be identified in regulatory impact analyses that accompany those regulations. The Department anticipates that such costs and savings will be relatively small compared to the privacy and Transactions rules. The Department anticipates that the net economic impact of the rules will be a net savings to the health care system.

[37] Health spending projections from *National Health Expenditure Projections 1998–2008* (January 2000), Health Care Financing Administration, Office of the Actuary, <*http://hcfa.hhs.gov/stats/nhe-proj/*>.