disclosures for health care operations, not for oversight purposes.

When they are performing accreditation activities for a covered entity, private accrediting organizations will meet the definition of business associate, and the covered entity must enter into a business associate contract with the accrediting organization in order to disclose protected health information. This is consistent with current practice; today, accrediting organizations perform their work pursuant to contracts with the accredited entity. This approach is also consistent with the recommendation by the Joint Commission on Accreditation of Healthcare Organizations and the National Committee for Quality Assurance, which stated in their report titled *Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment* (1998) that ''Oversight organizations, including accrediting bodies, states, and federal agencies, should include in their contracts terms that describe their responsibility to maintain the confidentiality of any personally identifiable health information that they review.''

We agree with the commenter who believed that private companies providing information to insurers and employers are not performing an oversight function; the definition of health oversight agency does not include such companies.

In developing and clarifying the definition of health oversight in the final rule, we seek to achieve a balance in accounting for the full range of activities that public agencies may undertake to perform their health oversight functions while establishing clear and appropriate boundaries on the definition so that it does not become a catch-all category that public and private agencies could use to justify any request for information.

Individual

Comment: A few commenters stated that foreign military and diplomatic personnel, and their dependents, and overseas foreign national beneficiaries, should not be excluded from the definition of ''individual.''

Response: We agree with concerns stated by commenters and eliminate these exclusions from the definition of ''individual'' in the final rule. Special rules for use and disclosure of protected health information about foreign military personnel are stated in § 164.512(k). Under the final rule, protected health information about diplomatic personnel is not accorded special treatment. While the exclusion of overseas foreign national beneficiaries has been deleted from the definition of ''individual,'' we have revised § 164.500 to indicate that the rule does not apply to the Department of Defense or other federal agencies or non-governmental organizations acting on its behalf when providing health care to overseas foreign national beneficiaries. This means that the rule will not cover any health information created incident to the provision of health care to foreign nationals overseas by U.S. sponsored missions or operations. (See § 164.500 and its corresponding preamble for details and the rationale for this policy.)

Comment: Several commenters expressed concern about the interrelationship of the definition of ''individual'' and the two year privacy protection for deceased persons.

Response: In the final rule, we eliminate the two year limit on privacy protection for protected health information about deceased individuals and require covered entities to comply with the requirements of the rule with respect to the protected health information of deceased individuals as long as they hold such information. See discussion under § 164.502.

Individually Identifiable Health Information

Comment: A number of commenters suggested that HHS revise the definitions of health information and individually identifiable health information to include consistent language in paragraph (1) of each respective definition. They observed that paragraph (1) of the definition of health information reads: ''(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse * * *;'' in contrast to paragraph (1) of the definition of individually identifiable health information, which reads: ''(1) Is created by or received from a health care provider, health plan, employer, or health care clearinghouse * * *'' [Emphasis added.]

Another commenter asked that we delete from the definition of health information, the words ''health or'' to make the definition more consistent with the definition of ''health care,'' as well as the words ''whether oral or.''

Response: We define these terms in the final rule as they are defined by Congress in sections 1171(4) and 1171(6) of the Act, respectively. We have, however, changed the word ''from'' in the definition of ''individually identifiable health information'' to conform to the statute.

Comment: Several commenters urged that the definition of individually identifiable health information include information created or received by a researcher. They reasoned that it is important to ensure that researchers using personally identifiable health information are subject to federal privacy standards. They also stated that if information created by a school regarding the health status of its students could be labeled ''health information,'' then information compiled by a clinical researcher regarding an individual also should be considered health information.

Response: We are restricted to the statutory limits of the terms. The Congress did not include information created or received by a researcher in either definition, and, consequently, we do not include such language in the rule's definitions.

Comment: Several commenters suggested modifying the definition of individually identifiable health information to state as a condition that the information provide a direct means of identifying the individual. They commented that the rule should support the need of those (*e.g.,* researchers) who need ''ready access to health information * * * that remains linkable to specific individuals.''

Response: The Congress included in the statutory definition of individually identifiable health information the modifier ''reasonable basis'' when describing the condition for determining whether information can be used to identify the individual. Congress thus intended to go beyond ''direct'' identification and to encompass circumstances in which a reasonable likelihood of identification exists. Even after removing ''direct'' or ''obvious'' identifiers of information, a risk or probability of identification of the subject of the information may remain; in some instances, the risk will not be inconsequential. Thus, we agree with the Congress that ''reasonable basis'' is the appropriate standard to adequately protect the privacy of individuals' health information.

Comment: A number of commenters suggested that the Secretary eliminate the distinction between protected health information and individually identifiable health information. One commenter asserted that all individually identifiable health information should be protected. One commenter observed that the terms individually identifiable health information and protected health information are defined differently in the rule and requested clarification as to the precise scope of coverage of the standards. Another commenter stated

that the definition of individually identifiable health information includes ''employer,'' whereas protected health information pertains only to covered entities for which employers are not included. The commenter argued that this was an ''incongruity'' between the definitions of individually identifiable health information and protected health information and recommended that we remove ''employer'' from the definition of individually identifiable health information.

Response: We define individually identifiable health information in the final rule generally as it is defined by Congress in section 1171(6) of the Act. Because ''employer'' is included in the statutory definition, we cannot accept the comment to remove the word ''employer'' from the regulatory definition.

We use the phrase 'protected health information' to distinguish between the individually identifiable health information that is used or disclosed by the entities that are subject to this rule and the entire universe of individually identifiable health information. 'Individually identifiable health information' as defined in the statute is not limited to health information used or disclosed by covered entities, so the qualifying phrase 'protected health information' is necessary to define that individually identifiable health information to which this rule applies.

Comment: One commenter noted that the definition of individually identifiable health information in the NPRM appeared to be the same definition used in the other HIPAA proposed rule, Security and Electronic Signature Standards (63 FR 43242). However, the commenter stated that the additional condition in the privacy NPRM, that protected health information is or has been electronically transmitted or electronically maintained by a covered entity and includes such information in any other form, appears to create potential disparity between the requirements of the two rules. The commenter questioned whether the provisions in proposed § 164.518(c) were an attempt to install similar security safeguards for such situations.

Response: The statutory definition of individually identifiable health information applies to the entire Administrative Simplification subtitle of HIPAA and, thus, was included in the proposed Security Standards. At this time, however, the final Security Standards have not been published, so the definition of protected health information is relevant only to HIPAA's privacy standards and is, therefore, included in subpart E of part 164 only. We clarify that the requirements in the proposed Security Standards are distinct and separate from the privacy safeguards promulgated in this final rule.

Comment: Several commenters expressed confusion and requested clarification as to what is considered health information or individually identifiable health information for purposes of the rule. For example, one commenter was concerned that information exists in collection agencies, credit bureaus, etc., which could be included under the proposed regulation but may or may not have been originally obtained by a covered entity. The commenter noted that generally this information is not clinical, but it could be inferred from the data that a health care provider provided a person or member of person's family with health care services. The commenter urged the Secretary to define more clearly what and when information is covered.

One commenter queried how a non-medical record keeper could tell when personal information is health information within the meaning of rule, *e.g.,* when a worker asks for a low salt meal in a company cafeteria, when a travel voucher of an employee indicates that the traveler returned from an area that had an outbreak of fever, or when an airline passenger requests a wheel chair. It was suggested that the rule cover health information in the hands of schools, employers, and life insurers only when they receive individually identifiable health information from a covered entity or when they create it while providing treatment or making payment.

Response: This rule applies only to individually identifiable health information that is held by a covered entity. Credit bureaus, airlines, schools, and life insurers are not covered entities, so the information described in the above comments is not protected health information. Similarly, employers are not covered entities under the rule. Covered entities must comply with this regulation in their health care capacity, not in their capacity as employers. For example, information in hospital personnel files about a nurses' sick leave is not protected health information under this rule.

Comment: One commenter recommended that the privacy of health information should relate to actual medical records. The commenter expressed concern about the definition's broadness and contended that applying prescriptive rules to information that health plans hold will not only delay processing of claims and coverage decisions, but ultimately affect the quality and cost of care for health care consumers.

Response: We disagree. Health information about individuals exists in many types of records, not just the formal medical record about the individual. Limiting the rule's protections to individually identifiable health information contained in medical records, rather than individually identifiable health information in any form, would omit a significant amount of individually identifiable health information, including much information in covered transactions.

Comment: One commenter voiced a need for a single standard for individually identifiable health information and disability and workers' compensation information; each category of information is located in their one electronic data base, but would be subjected to a different set of use and transmission rules.

Response: We agree that a uniform, comprehensive privacy standard is desirable. However, our authority under the HIPAA is limited to individually identifiable health information as it is defined in the statute. The legislative history of HIPAA makes clear that workers' compensation and disability benefits programs were not intended to be covered by the rule. Entities are of course free to apply the protections required by this rule to all health information they hold, including the excepted benefits information, if they wish to do so (for example, in order to reduce administrative burden).

Comment: Commenters recommended that the definition of individually identifiable health information not include demographic information that does not have any additional health, treatment, or payment information with it. Another commenter recommended that protected health information should not include demographic information at all.

Response: Congress explicitly included demographic information in the statutory definition of this term, so we include such language in our regulatory definition of it.

Comments: A number of commenters expressed concern about whether references to personal information about individuals, such as ''John Doe is fit to work as a pipe fitter * * *'' or ''Jane Roe can stand no more than 2 hours * * *'', would be considered individually identifiable health information. They argued that such ''fitness-to-work'' and ''fitness for duty'' statements are not health care because they do not reveal the type of

information (such as the diagnosis) that is detrimental to an individual's privacy interest in the work environment.

Response: References to personal information such as those suggested by the commenters could be individually identifiable health information if the references were created or received by a health care provider, health plan, employer, or health care clearinghouse and they related to the past, present, or future physical or mental health or condition, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. Although these fitness for duty statements may not reveal a diagnosis, they do relate to a present physical or mental condition of an individual because they describe the individual's capacity to perform the physical and mental requirements of a particular job at the time the statement is made (even though there may be other non-health-based qualifications for the job). If these statements were created or received by one of more of the entities described above, they would be individually identifiable health information.

Law Enforcement Official

Comment: Some commenters, particularly those representing health care providers, expressed concern that the proposed definition of ''law enforcement official'' could have allowed many government officials without health care oversight duties to obtain access to protected health information without patient consent.

Response: We do not intend for the definition of ''law enforcement official'' to be limited to officials with responsibilities directly related to health care. Law enforcement officials may need protected health information for investigations or prosecutions unrelated to health care, such as investigations of violent crime, criminal fraud, or crimes committed on the premises of health care providers. For these reasons, we believe it is not appropriate to limit the definition of ''law enforcement official'' to persons with responsibilities of oversight of the health care system.

Comment: A few commenters expressed concern that the proposed definition could include any county or municipal official, even those without traditional law enforcement training.

Response: We do not believe that determining training requirements for law enforcement officials is appropriately within the purview of this regulation; therefore, we do not make the changes that these commenters requested.

Comment: Some commenters, particularly those from the district attorney community, expressed general concern that the proposed definition of ''law enforcement official'' was too narrow to account for the variation in state interpretations of law enforcement officials' power. One group noted specifically that the proposed definition could have prevented prosecutors from gaining access to needed protected health information.

Response: We agree that protected health information may be needed by law enforcement officials for both investigations and prosecutions. We did not intend to exclude the prosecutorial function from the definition of ''law enforcement official,'' and accordingly we modify the definition of law enforcement official to reflect their involvement in prosecuting cases. Specifically, in the final rule, we define law enforcement official as an official of any agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to: (1) Investigate or conduct an inquiry into a potential violation of law; or (2) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Comment: One commenter recommended making the definition of law enforcement official broad enough to encompass Medicaid program auditors, because some matters requiring civil or criminal law enforcement action are first identified through the audit process.

Response: We disagree. Program auditors may obtain protected health information necessary for their audit functions under the oversight provision of this regulation (§ 164.512(d)).

Comment: One commenter suggested that the proposed definition of ''law enforcement official'' could be construed as limited to circumstances in which an official ''knows'' that law has been violated. This commenter was concerned that, because individuals are presumed innocent and because many investigations, such as random audits, are opened without an agency knowing that there is a violation, the definition would not have allowed disclosure of protected health information for these purposes. The commenter recommended modifying the definition to include investigations into ''whether'' the law has been violated.

Response: We do not intend for lawful disclosures of protected health information for law enforcement purposes to be limited to those in which a law enforcement official knows that law has been violated. Accordingly, we revise the definition of ''law enforcement official'' to include investigations of ''potential'' violations of law.

Marketing

Comments related to ''marketing'' are addressed in the responses to comments regarding § 164.514(e).

Payment

Comment: One commenter urged that the Department not permit protected health information to be disclosed to a collection agency for collecting payment on a balance due on patient accounts. The commenter noted that, at best, such a disclosure would only require the patient's and/or insured's address and phone number.

Response: We disagree. A collection agency may require additional protected health information to investigate and assess payment disputes for the covered entity. For example, the collection agency may need to know what services the covered entity rendered in order to resolve disputes about amounts due. The information necessary may vary, depending on the nature of the dispute. Therefore we do not specify the information that may be used or disclosed for collection activities. The commenter's concern may be addressed by the minimum necessary requirements in § 164.514. Under those provisions, when a covered entity determines that a collection agency only requires limited information for its activities, it must make reasonable efforts to limit disclosure to that information.

Comment: A number of commenters supported retaining the expansive definition in the proposed rule so that current methods of administering the claims payment process would not be hindered by blocking access to protected health information.

Response: We agree and retain the proposed overall approach to the definition.

Comment: Some commenters argued that the definition of ''payment'' should be narrowly interpreted as applying only to the individual who is the subject of the information.

Response: We agree with the commenter and modify the definition to clarify that payment activities relate to the individual to whom health care is provided.

Comment: Another group of commenters asserted that the doctor-patient relationship was already being interfered with by the current practices of managed care. For example, it was argued that the definition expanded the

power of government and other third party ''payors,'' turning them into controllers along with managed care companies. Others stated that activities provided for under the definition occur primarily to fulfill the administrative function of managed health plans and that an individual's privacy is lost when his or her individually identifiable health information is shared for administrative purposes.

Response: Activities we include in the definition of payment reflect core functions through which health care and health insurance services are funded. It would not be appropriate for a rule about health information privacy to hinder mechanisms by which health care is delivered and financed. We do not through this rule require any health care provider to disclose protected health information to governmental or other third party payors for the activities listed in the payment definition. Rather, we allow these activities to occur, subject to and consistent with the requirements of this rule.

Comment: Several commenters requested that we expand the definition to include ''coordination of benefits'' as a permissible activity.

Response: We agree and modify the definition accordingly.

Comment: A few commenters raised concerns that the use of ''medical data processing'' was too restrictive. It was suggested that a broader reference such as ''health related'' data processing would be more appropriate.

Response: We agree and modify the definition accordingly.

Comment: Some commenters suggested that the final rule needed to clarify that drug formulary administration activities are payment related activities.

Response: While we agree that uses and disclosures of protected health information for drug formulary administration and development are common and important activities, we believe these activities are better described as health care operations and that these activities come within that definition.

Comment: Commenters asked that the definition include calculation of prescription drug costs, drug discounts, and maximum allowable costs and copayments.

Response: Calculations of drug costs, discounts, or copayments are payment activities if performed with respect to a specific individual and are health care operations if performed in the aggregate for a group of individuals.

Comment: We were urged to specifically exclude ''therapeutic substitution'' from the definition.

Response: We reject this suggestion. While we understand that there are policy concerns regarding therapeutic substitution, those policy concerns are not primarily about privacy and thus are not appropriately addressed in this regulation.

Comment: A few commenters asked that patient assistance programs (PAPS) should be excluded from the definition of payment. Such programs are run by or on behalf of manufacturers and provide free or discounted medications to individuals who could not afford to purchase them. Commenters were concerned that including such activities in the definition of payment could harm these programs.

For example, a university school of pharmacy may operate an outreach program and serve as a clearinghouse for information on various pharmaceutical manufacturer PAPS. Under the program state residents can submit a simple application to the program (including medication regimen and financial information), which is reviewed by program pharmacists who study the eligibility criteria and/or directly call the manufacturer's program personnel to help evaluate eligibility for particular PAPS. The program provides written guidance to the prescribing physicians that includes a suggested approach for helping their indigent patients obtain the medications that they need and enrollment information for particular PAPS.

Response: We note that the concerns presented are not affected by definition of ''payment.'' The application of this rule to patient assistance programs activities will depend on how the individual programs operate and are affected primarily by the definition of treatment. Each of these programs function differently, so it is not possible to state a blanket rule for whether and how the rule affects such programs.

Under the example provided, the physician who contacts the program on behalf of a patient is managing the patient's care. If the provider is also a covered entity, he or she would be permitted to make such a ''treatment'' disclosure of protected health information if a general consent had been obtained from the patient. Depending on the particular facts, the manufacturer, by providing the prescription drugs for an individual, could also be providing health care under this rule. Even so, however, the manufacturer may or may not be a covered entity, depending on whether or not it engages in any of the standard electronic transactions (See the definition of a covered entity). It also may be an indirect treatment provider, since it may be providing the product through another provider, not directly to the patient. In this example, the relevant disclosures of protected health information by any covered health care provider with a direct treatment relationship with the patient would be permitted subject to the general consent requirements of § 164.506.

Whether and how this rule affects the school of pharmacy is equally dependent on the specific facts. For example, if the school merely provides a patient or a physician with the name of a manufacturer and a contact phone number, it would not be functioning as a health care provider and would not be subject to the rule. However, if the school is more involved in the care of the individual, its activities could come in within the definition of ''health care provider'' under this rule.

Comment: Commenters pointed out that drugs may or may not be ''covered'' under a plan. Individuals, on the other hand, may or may not be ''eligible'' for benefits under a plan. The definition should incorporate both terms to clarify that determinations of both coverage and eligibility are payment activities.

Response: We agree and modify the rule to include ''eligibility''.

Comment: Several commenters urged that ''concurrent and retrospective review'' were significant utilization review activities and should be incorporated.

Response: We agree and modify the definition accordingly.

Comment: Commenters noted that the proposed rule was not clear as to whether protected health information could be used to resolve disputes over coverage, including appeals or complaints regarding quality of care.

Response: We modify the definition of payment to include resolution of payment and coverage disputes; the final definition of payment includes ''the adjudication * * * of health benefit claims.'' The other examples provided by commenters, such as arranging, conducting, or assistance with primary and appellate level review of enrollee coverage appeals, also fall within the scope of adjudication of health benefits claims. Uses and disclosures of protected health information to resolve disputes over quality of care may be made under the definition of ''health care operations'' (see above).

Comment: Some commenters suggested that if an activity falls within the scope of payment it should not be considered marketing. Commenters supported an approach that would bar such an activity from being construed as ''marketing'' even if performing that

activity would result in financial gain to the covered entity.

Response: We agree that the proposed rule did not clearly define ''marketing,'' leaving commenters to be concerned about whether payment activities that result in financial gain might be considered marketing. In the final rule we add a definition of marketing and clarify when certain activities that would otherwise fall within that definition can be accomplished without authorization. We believe that these changes will clarify the distinction between marketing and payment and address the concerns raised by commenters.

Comment: Commenters asserted that HHS should not include long-term care insurance within the definition of ''health plan.'' If they are included, the commenters argued that the definition of payment must be modified to reflect the activities necessary to support the payment of long-term care insurance claims. As proposed, commenters argued that the definition of payment would not permit long term care insurers to use and disclose protected health information without authorization to perform functions that are ''compatible with and directly relate to * * * payment'' of claims submitted under long term care policies.

Response: Long-term care policies, except for nursing home fixed-indemnity policies, are defined as health plans by the statute (see definition of ''health plan,'' above). We disagree with the assertion that the definition of payment does not permit long term care insurers to undertake these necessary activities. Processing of premium payments, claims administration, and other activities suggested for inclusion by the commenters are covered by the definition. The rule permits protected health information to be used or disclosed by a health plan to determine or fulfill its responsibility for provision of benefits under the health plan.

Comment: Some commenters argued that the definition needs to be expanded to include the functions of obtaining stop-loss and ceding reinsurance.

Response: We agree that use and disclosure of protected health information for these activities should be permitted without authorization, but have included them under health care operation rather than payment.

Comment: Commenters asked that the definition be modified to include collection of accounts receivable or outstanding accounts. Commenters raised concern that the proposed rule, without changes, might unintentionally prevent the flow of information between medical providers and debt collectors.

Response: We agree that the proposed definition of payment did not explicitly provide for ''collection activities'' and that this oversight might have impeded a covered entity's debt collection efforts. We modify the regulatory text to add ''collection activities.''

Comment: The preamble should clarify that self-insured group health and workers' compensation plans are not covered entities or business partners.

Response: The statutory definition of health plan does not include workers' compensation products. See the discussion of ''health plan'' under § 160.103 above.

Comment: Certain commenters explained that third party administrators usually communicate with employees through Explanation of Benefit (EOB) reports on behalf of their dependents (including those who might not be minor children). Thus, the employee might be apprised of the medical encounters of his or her dependents but not of medical diagnoses unless there is an over-riding reason, such as a child suspected of drug abuse due to multiple prescriptions. The commenters urged that the current claim processing procedures be allowed to continue.

Response: We agree. We interpret the definition of payment and, in particular the term ''claims management,'' to include such disclosures of protected health information.

Comment: One private company noted that pursuant to the proposed Transactions Rule standard for payment and remittance advice, the ASC X12N 835 can be used to make a payment, send a remittance advice, or make a payment and send remittance advice by a health care payor and a health care provider, either directly or through a designated financial institution. Because a remittance advice includes diagnostic or treatment information, several private companies and a few public agencies believed that the proposed Transactions Rule conflicted with the proposed privacy rule. Two health plans requested guidance as to whether, pursuant to the ASC X12N 835 implementation guide, remittance advice information is considered ''required'' or ''situational.'' They sought guidance on whether covered entities could include benefits information in payment of claims and transfer of remittance information.

One commenter asserted that if the transmission of certain protected health information were prohibited, health plans may be required to strip remittance advice information from the ASC X12N 835 when making health care payments. It recommended modifying the proposed rule to allow covered entities to provide banks or financial institutions with the data specified in any transaction set mandated under the Transactions Rule for health care claims payment.

Similarly, a private company and a state health data organization recommended broadening the scope of permissible disclosures pursuant to the banking section to include integrated claims processing information, as contained in the ASC X12N 835 and proposed for adoption in the proposed Transactions Rule; this transaction standard includes diagnostic and treatment information. The company argued that inclusion of diagnostic and treatment information in the data transmitted in claims processing was necessary for comprehensive and efficient integration in the provider's patient accounting system of data corresponding with payment that financial institutions credit to the provider's account.

A state health data organization recommended applying these rules to financial institutions that process electronic remittance advice pursuant to the Transactions Rule.

Response: The Transactions Rule was published August 17, 2000, after the issuance of the privacy proposed rule. As noted by the commenters, the ASC X12N 835 we adopted as the ''Health Care Payment and Remittance Advice'' standard in the Transactions Rule has two parts. They are the electronic funds transfer (EFT) and the electronic remittance advice (ERA). The EFT part is optional and is the mechanism that payors use to electronically instruct one financial institution to move money from one account to another at the same or at another financial institution. The EFT includes information about the payor, the payee, the amount, the payment method, and a reassociation trace number. Since the EFT is used to initiate the transfer of funds between the accounts of two organizations, typically a payor to a provider, it includes no individually identifiable health information, not even the names of the patients whose claims are being paid. The funds transfer information may also be transmitted manually (by check) or by a variety of other electronic means, including various formats of electronic transactions sent through a payment network, such as the Automated Clearing House (ACH) Network.

The ERA, on the other hand, contains specific information about the patients and the medical procedures for which

the money is being paid and is used to update the accounts receivable system of the provider. This information is always needed to complete a standard Health Care Payment and Remittance Advice transaction, but is never needed for the funds transfer activity of the financial institution. The only information the two parts of this transaction have in common is the reassociation trace number.

Under the ASC X12N 835 standard, the ERA may be transmitted alone, directly from the health plan to the health care provider and the reassociation trace number is used by the provider to match the ERA information with a specific payment conducted in some other way (e.g., EFT or paper check). The standard also allows the EFT to be transmitted alone, directly to the financial institution that will initiate the payment. It also allows both parts to be transmitted together, even though the intended recipients of the two parts are different (the financial institution and the provider). For example, this would be done when the parties agree to use the ACH system to carry the ERA through the provider's bank to the provider when it is more efficient than sending the ERA separately through a different electronic medium.

Similarly, the ASC X12N 820 standard for premium payments has two parts, an EFT part (identical to that of the 835) and a premium data part containing identity and health information about the individuals for whom health insurance premiums are being paid.

The transmission of both parts of the standards are payment activities under this rule, and permitted subject to certain restrictions. Because a financial institution does not require the remittance advice or premium data parts to conduct funds transfers, disclosure of those parts by a covered entity to it (absent a business associate arrangement to use the information to conduct other activities) would be a violation of this rule.

We note that additional requirements may be imposed by the final Security Rule. Under the proposed Security Rule, the ACH system and similar systems would have been considered ''open networks'' because transmissions flow unpredictably through and become available to member institutions who are not party to any business associate agreements (in a way similar to the internet). The proposed Security Rule would require any protected health information transferred through the ACH or similar system to be encrypted.

Comment: A few commenters noted the Gramm-Leach-Bliley (GLB) Act (Pub. L. 106–102) allows financial holding companies to engage in a variety of business activities, such as insurance and securities, beyond traditional banking activities. Because the term ''banking'' may take on broader meaning in light of these changes, the commenter recommended modifying the proposed rule to state that disclosure of diagnostic and treatment information to banks along with payment information would constitute a violation of the rule. Specifically, the organization recommended clarifying in the final rule that the provisions included in the proposed section on banking and payment processes (proposed § 164.510(i)) govern payment processes only and that all activities of financial institutions that did not relate directly to payment processes must be conducted through business partner contracts. Furthermore, this group recommended clarifying that if financial institutions act as payors, they will be covered entities under the rule.

Response: We recognize that implementation of the GLB Act will expand significantly the scope of activities in which financial holding companies engage. However, unless a financial institution also meets the definition of a ''covered entity,'' it cannot be a covered entity under this rule.

We agree with the commenters that disclosure of diagnostic and specific treatment information to financial institutions for many banking and funds processing purposes may not be consistent with the minimum necessary requirements of this final rule. We also agree with the commenters that financial institutions are business associates if they receive protected health information when they engage in activities other than funds processing for covered entities. For example, if a health care provider contracts with a financial institution to conduct ''back office'' billing and accounts receivable activities, we require the provider to enter into a business associate contract with the institution.

Comment: Two commenters expressed support for the proposed rule's approach to disclosure for banking and payment processes. On the other hand, many other commenters were opposed to disclosure of protected health information without authorization to banks. One commenter said that no financial institution should have individually identifiable health information for any reason, and it said there were technological means for separating identity from information necessary for financial transactions. Some commenters believed that implementation of the proposed rule's banking provisions could lead banks to deny loans on the basis of individuals' health information.

Response: We seek to achieve a balance between protecting patient privacy and facilitating the efficient operation of the health care system. While we agree that financial institutions should not have access to extensive information about individuals' health, we recognize that even the minimal information required for processing of payments may effectively reveal a patient's health condition; for example, the fact that a person has written a check to a provider suggests that services were rendered to the person or a family member. Requiring authorization for disclosure of protected health information to a financial institution in order to process every payment transaction in the health care system would make it difficult, if not impossible, for the health care system to operate effectively. See also discussion of section 1179 of the Act above.

Comment: Under the proposed rule, covered entities could have disclosed the following information without consent to financial institutions for the purpose of processing payments: (1) The account holder's name and address; (2) the payor or provider's name and address; (3) the amount of the charge for health services; (4) the date on which services were rendered; (5) the expiration date for the payment mechanism, if applicable (e.g., credit card expiration date); and (6) the individual's signature. The proposed rule solicited comments on whether additional data elements would be necessary to process payment transactions from patients to covered entities.

One commenter believed that it was unnecessary to include this list in the final rule, because information that could have been disclosed under the proposed minimum necessary rule would have been sufficient to process banking and payment information. Another private company said that its extensive payment systems experience indicated that we should avoid attempts to enumerate a list of information allowed to be disclosed for banking and payment processing. Furthermore, the commenter said, the proposed rule's list of information allowed to be disclosed was not sufficient to perform the range of activities necessary for the operation of modern electronic payment systems. Finally, the commenter said, inclusion of specific data elements allowed to be

disclosed for banking and payment processes rule would stifle innovation in continually evolving payment systems. Thus, the commenter recommended that in the final rule, we eliminate the minimum necessary requirement for banking and payment processing and that we do not include a list of specific types of information allowed to be disclosed for banking and payment processes.

On the other hand, several other commenters supported applying the minimum necessary standard to covered entities' disclosures to financial institutions for payment processing. In addition, these groups said that because financial institutions are not covered entities under the proposed rule, they urged Congress to enact comprehensive privacy legislation to limit financial institutions' use and re-disclosure of the minimally necessary protected health information they could receive under the proposed rule. Several of these commenters said that, in light of the increased ability to manipulate data electronically, they were concerned that financial institutions could use the minimal protected health information they received for making financial decisions. For example, one of these commenters said that a financial institution could identify an individual who had paid for treatment of domestic violence injuries and subsequently could deny the individual a mortgage based on that information.

Response: We agree with the commenters who were concerned that a finite list of information could hamper systems innovation, and we eliminate the proposed list of data items. However, we disagree with the commenters who argued that the requirement for minimum necessary disclosures not apply to disclosures to financial institution or for payment activities. They presented no persuasive reasons why these disclosures differ from others to which the standard applies, nor did they suggest alternative means of protecting individuals' privacy. Further, with elimination of the proposed list of items that may be disclosed, it will be necessary to rely on the minimum necessary disclosure requirement to ensure that disclosures for payment purposes do not include information unnecessary for that purposes. In practice, the following is the information that generally will be needed: the name and address of the individual; the name and address of the payor or provider; the amount of the charge for health services; the date on which health services were rendered; the expiration date for the payment mechanism, if applicable (i.e., credit card expiration date); the individual's signature; and relevant identification and account numbers.

Comment: One commenter said that the minimum necessary standard would be impossible to implement with respect to information provided on its standard payment claim, which, it said, was used by pharmacies for concurrent drug utilization review and that was expected to be adopted by HHS as the national pharmacy payment claim.

Two other commenters also recommended clarifying in the final rule that pharmacy benefit cards are not considered a type of ''other payment card'' pursuant to the rule's provisions governing payment processes. These commenters were concerned that if pharmacy benefit cards were covered by the rule's payment processing provisions, their payment claim, which they said was expected to be adopted by HHS as the national pharmacy payment claim, may have to be modified to comply with the minimum necessary standard that would have been required pursuant to proposed § 164.510(i) on banking and payment processes. One of these commenters noted that its payment claim facilitates concurrent drug utilization review, which was mandated by Congress pursuant to the Omnibus Budget Reconciliation Act of 1990 and which creates the real-time ability for pharmacies to gain access to information that may be necessary to meet requirements of this and similar state laws. The commenter said that information on its standard payment claim may include information that could be used to provide professional pharmacy services, such as compliance, disease management, and outcomes programs. The commenter opposed restricting such information by applying the minimum necessary standard.

Response: We make an exception to the minimum necessary disclosure provision of this rule for the required and situational data elements of the standard transactions adopted in the Transactions Rule, because those elements were agreed to through the ANSI-accredited consensus development process. The minimum necessary requirements do apply to optional elements in such standard transactions, because industry consensus has not resulted in precise and unambiguous situation specific language to describe their usage. This is particularly relevant to the NCPDP standards for retail pharmacy transactions referenced by these commenters, in which the current standard leaves most fields optional. For this reason, we do not accept this suggestion.

The term 'payment card' was intended to apply to a debit or credit card used to initiate payment transactions with a financial institution. We clarify that pharmacy benefit cards, as well as other health benefit cards, are used for identification of individual, plan, and benefits and do not qualify as ''other payment cards.''

Comment: Two commenters asked the following questions regarding the banking provisions of the proposed rule: (1) Does the proposed regulation stipulate that disclosures to banks and financial institutions can occur only once a patient has presented a check or credit card to the provider, or pursuant to a standing authorization?; and (2) Does the proposed rule ban disclosure of diagnostic or other related detailed payment information to financial institutions?

Response: We do not ban disclosure of diagnostic information to financial institutions, because some such information may be evident simply from the name of the payee (e.g., when payment is made to a substance abuse clinic). This type of disclosure, however, is permitted only when reasonably necessary for the transaction (see requirements for minimum necessary disclosure of protected health information, in § 164.502 and § 164.514).

Similarly, we do not stipulate that such disclosure may be made only once a patient has presented a check or credit card, because some covered entities hire financial institutions to perform services such as management of accounts receivables and other back office functions. In providing such services to covered entities, the financial institution will need access to protected health information. (In this situation, the disclosure will typically be made under a business associate arrangement that includes provisions for protection of the information.)

Comment: One commenter was concerned that the proposed rule's section on financial institutions, when considered in conjunction with the proposed definition of ''protected health information,'' could have been construed as making covered entities' disclosures of consumer payment history information to consumer reporting agencies subject to the rule. It noted that covered entities' reporting of payment history information to consumer reporting agencies was not explicitly covered by the proposed rule's provisions regarding disclosure of protected health information without authorization. It was also concerned that the proposed rule's minimum necessary standard could have been interpreted to

prevent covered entities and their business partners from disclosing appropriate and complete information to consumer reporting agencies. As a result, it said, consumer reporting agencies might not be able to compile complete consumer reports, thus potentially creating an inaccurate picture of a consumer's credit history that could be used to make future credit decisions about the individual.

Furthermore, this commenter said, the proposed rule could have been interpreted to apply to any information disclosed to consumer reporting agencies, thus creating the possibility for conflicts between the rule's requirements and those of the Fair Credit Reporting Act. They indicated that areas of potential overlap included: limits on subsequent disclosures; individual access rights; safeguards; and notice requirements.

Response: We have added to the definition of ''payment'' disclosure of certain information to consumer reporting agencies. With respect to the remaining concerns, this rule does not apply to consumer reporting agencies if they are not covered entities.

Comment: Several commenters recommended prohibiting disclosure of psychotherapy notes under this provision and under all of the sections governing disclosure without consent for national priority purposes.

Response: We agree that psychotherapy notes should not be disclosed without authorization for payment purposes, and the final rule does not allow such disclosure. See the discussion under § 164.508.

Protected Health Information

Comment: An overwhelmingly large number of commenters urged the Secretary to expand privacy protection to all individually identifiable health information, regardless of form, held or transmitted by a covered entity. Commenters provided many arguments in support of their position. They asserted that expanding the scope of covered information under the rule would increase patient confidence in their health care providers and the health care system in general. Commenters stated that patients may not seek care or honestly discuss their health conditions with providers if they do not believe that all of their health information is confidential. In particular, many suggested that this fear would be particularly strong with certain classes of patients, such as persons with disabilities, who may be concerned about potential discrimination, embarrassment or stigmatization, or domestic violence victims, who may hide the real cause of their injuries.

In addition, commenters felt that a more uniform standard that covered all records would reduce the complexity, burden, cost, and enforcement problems that would result from the NPRM's proposal to treat electronic and non-electronic records differently. Specifically, they suggested that such a standard would eliminate any confusion regarding how to treat mixed records (paper records that include information that has been stored or transmitted electronically) and would eliminate the need for health care providers to keep track of which portions of a paper record have been (or will be) stored or transmitted electronically, and which are not. Many of these commenters argued that limiting the definition to information that is or has at one time been electronic would result in different protections for electronic and paper records, which they believe would be unwarranted and give consumers a false sense of security. Other comments argued that the proposed definition would cause confusion for providers and patients and would likely cause difficulties in claims processing. Many others complained about the difficulty of determining whether information has been maintained or transmitted electronically. Some asked us to explicitly list the electronic functions that are intended to be excluded, such as voice mail, fax, etc. It was also recommended that the definitions of ''electronic transmission'' and ''electronic maintenance'' be deleted. It was stated that the rule may apply to many medical devices that are regulated by the FDA. A commenter also asserted that the proposal's definition was technically flawed in that computers are also involved in analog electronic transmissions such as faxes, telephone, etc., which is not the intent of the language. Many commenters argued that limiting the definition to information that has been electronic would create a significant administrative burden, because covered entities would have to figure out how to apply the rule to some but not all information.

Others argued that covering all individually identifiable health information would eliminate any disincentives for covered entities to convert from paper to computerized record systems. These commenters asserted that under the proposed limited coverage, contrary to the intent of HIPAA's administrative simplification standards, providers would avoid converting paper records into computerized systems in order to bypass the provisions of the regulation. They argued that treating all records the same is consistent with the goal of increasing the efficiency of the administration of health care services.

Lastly, in the NPRM, we explained that while we chose not to extend our regulatory coverage to all records, we did have the authority to do so. Several commenters agreed with our interpretation of the statute and our authority and reiterated such statements in arguing that we should expand the scope of the rule in this regard.

Response: We find these commenters' arguments persuasive and extend protections to individually identifiable health information transmitted or maintained by a covered entity in any form (subject to the exception for ''education records'' governed by FERPA and records described at 20 U.S.C. 1232g(a)(4)(B)(iv)). We do so for the reasons described by the commenters and in our NPRM, as well as because we believe that the approach in the final rule creates a logical, consistent system of protections that recognizes the dynamic nature of health information use and disclosure in a continually shifting health care environment. Rules that are specific to certain formats or media, such as ''electronic'' or ''paper,'' cannot address the privacy threats resulting from evolving forms of data capture and transmission or from the transfer of the information from one form to another. This approach avoids the somewhat artificial boundary issues that stem from defining what is and is not electronic.

In addition, we have reevaluated our reasons for not extending privacy protections to all paper records in the NPRM and after review of comments believe such justifications to be less compelling than we originally thought. For example, in the NPRM, we explained that we chose not to cover all paper records in order to focus on the public concerns about health information confidentiality in electronic communications, and out of concern that the potential additional burden of covering all records may not be justified because of the lower privacy risks presented by records that are in paper form only. As discussed above however, a great many commenters asserted that dealing with a mixture of protected and non-protected records is more burdensome, and that public concerns over health information confidentiality are not at all limited to electronic communications.

We note that medical devices in and of themselves, for example, pacemakers, are not protected health information for purposes of this regulation. However, information in or from the device may

be protected health information to the extent that it otherwise meets the definition.

Comment: Numerous commenters argued that the proposed coverage of any information other than that which is transmitted electronically and/or in a HIPAA transaction exceeds the Secretary's authority under section 264(c)(1) of HIPAA. The principal argument was that the initial language in section 264(c)(1) (''If language 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 * * * is not enacted by [August 21, 1999], the Secretary * * * shall promulgate final regulations containing such standards* * *'') limits the privacy standards to ''information transmitted in connection with the [HIPAA] transactions.'' The precise argument made by some commenters was that the grant of authority is contained in the words ''such standards,'' and that the referent of that phrase was ''standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a)* * *''.

Commenters also argued that this limitation on the Secretary's authority is discernible from the statutory purpose statement at section 261 of HIPAA, from the title to section 1173(a) (''Standards to Enable Electronic Exchange''), and from various statements in the legislative history, such as the statement in the Conference Report that the ''Secretary would be required to establish standards and modifications to such standards regarding the privacy of individually identifiable health information that is in the health information network.'' H. Rep. No. 104–736,104th Cong., 2d Sess., at 265. It was also argued that extension of coverage beyond the HIPAA transactions would be inconsistent with the underlying statutory trade-off between facilitating accessibility of information in the electronic transactions for which standards are adopted under section 1173(a) and protecting that information through the privacy standards.

Other commenters argued more generally that the Secretary's authority was limited to information in electronic form only, not information in any other form. These comments tended to focus on the statutory concern with regulating transactions in electronic form and argued that there was no need to have the privacy standards apply to information in paper form, because there is significantly less risk of breach of privacy with respect to such information.

The primary justifications provided by commenters for restricting the scope of covered individually identifiable health information under the regulation were that such an approach would reduce the complexity, burden, cost, and enforcement problems that would result from a rule that treats electronic and non-electronic records differently; would appropriately limit the rule's focus to the security risks that are inherent in electronic transmission or maintenance of individually identifiable health information; and would conform these provisions of the rule more closely with their interpretation of the HIPAA statutory language.

Response: We disagree with these commenters. We believe that restricting the scope of covered information under the rule consistent with any of the comments described above would generate a number of policy concerns. Any restriction in the application of privacy protections based on the media used to maintain or transmit the information is by definition arbitrary, unrelated to the potential use or disclosure of the information itself and therefore not responsive to actual privacy risks. For example, information contained in a paper record may be scanned and transmitted worldwide almost as easily as the same information contained in an electronic claims transaction, but would potentially not be protected.

In addition, application of the rule to only the standard transactions would leave large gaps in the amount of health information covered. This limitation would be particularly harmful for information used and disclosed by health care providers, who are likely to maintain a great deal of information never contained in a transaction.

We disagree with the arguments that the Secretary lacks legal authority to cover all individually identifiable health information transmitted or maintained by covered entities. The arguments raised by these comments have two component parts: (1) That the Secretary's authority is limited by form, to individually identifiable health information in electronic form only; and (2) that the Secretary's authority is limited by content, to individually identifiable health information that is contained in what commenters generally termed the ''HIPAA transactions,'' i.e., information contained in a transaction for which a standard has been adopted under section 1173(a) of the Act.

With respect to the issue of form, the statutory definition of ''health information'' at section 1171(4) of the Act defines such information as ''any information, *whether oral or recorded in any form or medium*'' (emphasis added) which is created or received by certain entities and relates to the health condition of an individual or the provision of health care to an individual (emphasis added). ''Individually identifiable health information'', as defined at section 1171(6) of the Act, is information that is created or received by a subset of the entities listed in the definition of ''health information'', relates to the same subjects as ''health information,'' and is, in addition, individually identifiable. Thus, ''individually identifiable health information'' is, as the term itself implies, a subset of ''health information.'' As ''health information,'' ''individually identifiable health information'' means, among other things, information that is ''oral or recorded in any form or medium.'' Therefore, the statute does not limit ''individually identifiable health information'' to information that is in electronic form only.

With respect to the issue of content, the limitation of the Secretary's authority to information in HIPAA transactions under section 264(c)(1) is more apparent than real. While the first sentence of section 264(c)(1) may be read as limiting the regulations to standards with respect to the privacy of individually identifiable health information ''transmitted in connection with the [HIPAA] transactions,'' what that sentence in fact states is that the privacy regulations must ''contain'' such standards, not be limited to such standards. The first sentence thus sets a statutory minimum, first for Congress, then for the Secretary. The second sentence of section 264(c)(1) directs that the regulations ''address at least the subjects in subsection (b) (of section 264).'' Section 264(b), in turn, refers only to ''individually identifiable health information'', with no qualifying language, and refers back to subsection (a) of section 264, which is not limited to HIPAA transactions. Thus, the first and second sentences of section 264(c)(1) can be read as consistent with each other, in which case they direct the issuance of privacy standards with respect to individually identifiable health information. Alternatively, they can be read as ambiguous, in which case one must turn to the legislative history.

The legislative history of section 264 does not reflect the content limitation of the first sentence of section 264(c)(1). Rather, the Conference Report

summarizes this section as follows: ''If Congress fails to enact privacy legislation, the Secretary is required to develop standards with respect to privacy of individually identifiable health information not later than 42 months from the date of enactment.'' *Id.*, at 270. This language indicates that the overriding purpose of section 264(c)(1) was to postpone the Secretary's duty to issue privacy standards (which otherwise would have been controlled by the time limits at section 1174(a)), in order to give Congress more time to pass privacy legislation. A corollary inference, which is also supported by other textual evidence in section 264 and Part C of title XI, is that if Congress failed to act within the time provided, the original statutory scheme was to kick in. Under that scheme, which is set out in section 1173(e) of the House bill, the standards to be adopted were ''standards with respect to the privacy of individually identifiable health information.'' Thus, the legislative history of section 264 supports the statutory interpretation underlying the rules below.

Comment: Many commenters were opposed to the rule covering specific forms of communication or records that could potentially be considered covered information, i.e., faxes, voice mail messages, etc. A subset of these commenters took issue particularly with the inclusion of oral communications within the scope of covered information. The commenters argued that covering information when it takes oral form (e.g., verbal discussions of a submitted claim) makes the regulation extremely costly and burdensome, and even impossible to administer. Another commenter also offered that it would make it nearly impossible to discuss health information over the phone, as the covered entity cannot verify that the person on the other end is in fact who he or she claims to be.

Response: We disagree. Covering oral communications is an important part of keeping individually identifiable health information private. If the final rule were not to cover oral communication, a conversation about a person's protected health information could be shared with anyone. Therefore, the same protections afforded to paper and electronically based information must apply to verbal communication as well. Moreover, the Congress explicitly included ''oral'' information in the statutory definition of health information.

Comment: A few commenters supported, without any change, the approach proposed in the NPRM to limit the scope of covered information to individually identifiable health information in any form once the information is transmitted or maintained electronically. These commenters asserted that our statutory authority limited us accordingly. Therefore, they believed we had proposed protections to the extent possible within the bounds of our statutory authority and could not expand the scope of such protections without new legislative authority.

Response: We disagree with these commenters regarding the limitations under our statutory authority. As explained above, we have the authority to extend the scope of the regulation as we have done in the final rule. We also note here that most of these commenters who supported the NPRM's proposed approach, voiced strong support for extending the scope of coverage to all individually identifiable health information in any form, but concluded that we had done what we could within the authority provided.

Comment: One commenter argued that the term ''transaction'' is generally understood to denote a business matter, and that the NPRM applied the term too broadly by including hospital directory information, communication with a patient's family, researchers' use of data and many other non-business activities.

Response: This comment reflects a misunderstanding of our use of the term ''transaction.'' The uses and disclosures described in the comment are not ''transactions'' as defined in § 160.103. The authority to regulate the types of uses and disclosures described is provided under section 264 of Pub. L. 104–191. The conduct of the activities noted by the commenters are not related to the determination of whether a health care provider is a covered entity. We explain in the preamble that a health care provider is a covered entity if it transmits health information in electronic form in connection with transactions referred to in section 1173(a)(1) of the Act.

Comment: A few commenters asserted that the Secretary has no authority to regulate ''use'' of protected health information. They stated that although section 264(b) mentions that the Secretary should address ''uses and disclosures,'' no other section of HIPAA employs the term ''use.''

Response: We disagree with these commenters. As they themselves note, the authority to regulate use is given in section 264(b) and is sufficient.

Comment: Some commenters requested clarification as to how certain types of health information, such as photographs, faxes, X-Rays, CT-scans, and others would be classified as protected or not under the rule.

Response: All types of individually identifiable health information in any form, including those described, when maintained or transmitted by a covered entity are covered in the final rule.

Comment: A few commenters requested clarification with regard to the differences between the definitions of individually identifiable health information and protected health information.

Response: In expanding the scope of covered information in the final rule, we have simplified the distinction between the two definitions. In the final rule, protected health information is the subset of individually identifiable health information that is maintained or transmitted by covered entity, and thereby protected by this rule. For additional discussion of protected health information and individually identifiable health information, see the descriptive summary of § 164.501.

Comment: A few commenters remarked that the federal government has no right to access or control any medical records and that HHS must get consent in order to store or use any individually identifiable health information.

Response: We understand the commenters' concern. It is not our intent, nor do we through this rule create any government right of access to medical records, except as needed to investigate possible violations of the rule. Some government programs, such as Medicare, are authorized under other law to gain access to certain beneficiary records for administrative purposes. However, these programs are covered by the rule and its privacy protections apply.

Comment: Some commenters asked us to clarify how schools would be treated by the rule. Some of these commenters worried that privacy would be compromised if schools were exempted from the provisions of the final rule. Other commenters thought that school medical records were included in the provisions of the NPRM.

Response: We agree with the request for clarification and provide guidance regarding the treatment of medical records in schools in the ''Relationship to Other Federal Laws'' preamble discussion of FERPA, which governs the privacy of education records.

Comment: One commenter was concerned that only some information from a medical chart would be included as covered information. The commenter was especially concerned that transcribed material might not be considered covered information.

Response: As stated above, all individually identifiable health information in any form, including transcribed or oral information, maintained or transmitted by a covered entity is covered under the provisions of the final rule.

Comment: In response to our solicitation of comments on the scope of the definition of protected health information, many commenters asked us to narrow the scope of the proposed definition to include only information in electronic form. Others asked us to include only information from the HIPAA standard transactions.

Response: For the reasons stated by the commenters who asked us to expand the proposed definition, we reject these comments. We reject these approaches for additional reasons, as well. Limiting the protections to electronic information would, in essence, protect information only as long as it remained in a computer or other electronic media; the protections in the rule could be avoided simply by printing out the information. This approach would thus result in the illusion, but not the reality, of privacy protections. Limiting protection to information in HIPAA transactions has many of the problems in the proposed approach: it would fail to protect significant amounts of health information, would force covered entities to figure out which information had and had not been in such a transaction, and could cause the administrative burdens the commenters feared would result from protecting some but not all information.

Comment: A few commenters asserted that the definition of protected health information should explicitly include ''genetic'' information. It was argued that improper disclosure and use of such information could have a profound impact on individuals and families.

Response: We agree that the definition of protected health information includes genetic information that otherwise meets the statutory definition. But we believe that singling out specific types of protected health information for special mention in the regulation text could wrongly imply that other types are not included.

Comment: One commenter recommended that the definition of protected health information be modified to clarify that an entity does not become a 'covered entity' by providing a device to an individual on which protected health information may be stored, provided that the company itself does not store the individual's health information.''

Response: We agree with the commenter's analysis, but believe the definition is sufficiently clear without a specific amendment to this effect.

Comment: One commenter recommended that the definition be amended to explicitly exclude individually identifiable health information maintained, used, or disclosed pursuant to the Fair Credit Reporting Act, as amended, 15 U.S.C. 1681. It was stated that a disclosure of payment history to a consumer reporting agency by a covered entity should not be considered protected health information. Another commenter recommended that health information, billing information, and a consumer's credit history be exempted from the definition because this flow of information is regulated by both the Fair Credit Reporting Act (FCRA) and the Fair Debt Collection Practices Act (FDCPA).

Response: We disagree. To the extent that such information meets the definition of protected health information, it is covered by this rule. These statutes are designed to protect financial, not health, information. Further, these statutes primarily regulate entities that are not covered by this rule, minimizing the potential for overlap or conflict. The protections in this rule are more appropriate for protecting health information. However, we add provisions to the definition of payment which should address these concerns. See the definition of 'payment' in § 164.501.

Comment: An insurance company recommended that the rule require that medical records containing protected health information include a notation on a cover sheet on such records.

Response: Since we have expanded the scope of protected health information, there is no need for covered entities to distinguish among their records, and such a notation is not needed. This uniform coverage eliminates the mixed record problem and resultant potential for confusion.

Comment: A government agency requested clarification of the definition to address the status of information that flows through dictation services.

Response: A covered entity may disclose protected health information for transcription of dictation under the definition of health care operations, which allows disclosure for ''general administrative'' functions. We view transcription and clerical services generally as part of a covered entity's general administrative functions. An entity transcribing dictation on behalf of a covered entity meets this rule's definition of business associate and may receive protected health information under a business associate contract with the covered entity and subject to the other requirements of the rule.

Comment: A commenter recommended that information transmitted for employee drug testing be exempted from the definition.

Response: We disagree that is necessary to specifically exclude such information from the definition of protected health information. If a covered entity is involved, triggering this rule, the employer may obtain authorization from the individuals to be tested. Nothing in this rule prohibits an employer from requiring an employee to provide such an authorization as a condition of employment.

Comment: A few commenters addressed our proposal to exclude individually identifiable health information in education records covered by FERPA. Some expressed support for the exclusion. One commenter recommended adding another exclusion to the definition for the treatment records of students who attend institutions of post secondary education or who are 18 years old or older to avoid confusion with rules under FERPA. Another commenter suggested that the definition exclude health information of participants in ''Job Corps programs'' as it has for educational records and inmates of correctional facilities.

Response: We agree with the commenter on the potential for confusion regarding records of students who attend post-secondary schools or who are over 18, and therefore in the final rule we exclude records defined at 20 U.S.C. 1232g(a)(4)(B)(iv) from the definition of protected health information. For a detailed discussion of this change, refer to the ''Relationship to Other Federal Laws'' section of the preamble. We find no similar reason to exclude ''Job Corps programs'' from the requirements of this regulation.

Comment: Some commenters voiced support for the exclusion of the records of inmates from the definition of protected health information, maintaining that correctional agencies have a legitimate need to share some health information internally without authorization between health service units in various facilities and for purposes of custody and security. Other commenters suggested that the proposed exclusion be extended to individually identifiable health information: created by covered entities providing services to inmates or detainees under contract to such facilities; of ''former'' inmates; and of persons who are in the custody of law enforcement officials, such as the United States Marshals Service and local police agencies. They stated that

corrections and detention facilities must be able to share information with law enforcement agencies such as the United States Marshals Service, the Immigration and Naturalization Services, county jails, and U.S. Probation Offices.

Another commenter said that there is a need to have access to records of individuals in community custody and explained that these individuals are still under the control of the state or local government and the need for immediate access to records for inspections and/or drug testing is necessary.

A number of commenters were opposed to the proposed exclusion to the definition of protected health information, arguing that the proposal was too sweeping. Commenters stated that while access without consent is acceptable for some purposes, it is not acceptable in all circumstances. Some of these commenters concurred with the sharing of health care information with other medical facilities when the inmate is transferred for treatment. These commenters recommended that we delete the exception for jails and prisons and substitute specific language about what information could be disclosed and the limited circumstances or purposes for which such disclosures could occur.

Others recommended omission of the proposed exclusion entirely, arguing that excluding this information from protection sends the message that, with respect to this population, abuses do not matter. Commenters argued that inmates and detainees have a right to privacy of medical records and that individually identifiable health information obtained in these settings can be misused, e.g., when communicated indiscriminately, health information can trigger assaults on individuals with stigmatized conditions by fellow inmates or detainees. It can also lead to the denial of privileges, or inappropriately influence the deliberations of bodies such as parole boards.

A number of commenters explicitly took issue with the exclusion relative to individuals, and in particular youths, with serious mental illness, seizure disorders, and emotional or substance abuse disorders. They argued that these individuals come in contact with criminal justice authorities as a result of behaviors stemming directly from their illness and assert that these provisions will cause serious problems. They argue that disclosing the fact that an individual was treated for mental illness while incarcerated could seriously impair the individual's reintegration into the community. Commenters stated that such disclosures could put the individual or family members at risk of discrimination by employers and in the community at large.

Some commenters asserted that the rule should be amended to prohibit jails and prisons from disclosing private medical information of individuals who have been discharged from these facilities. They argued that such disclosures may seriously impair individuals' rehabilitation into society and subject them to discrimination as they attempt to re-establish acceptance in the community.

Response: We find commenters' arguments against a blanket exemption from privacy protection for inmates persuasive. We agree health information in these settings may be misused, which consequently poses many risks to the inmate or detainee and in some cases, their families as described above by the commenters. Accordingly, we delete this exception from the definition of ''protected health information'' in the final rule. The final rule considers individually identifiable health information of individuals who are prisoners and detainees to be protected health information to the extent that it meets the definition and is maintained or transmitted by a covered entity.

At the same time, we agree with those commenters who explained that correctional facilities have legitimate needs for use and sharing of individually identifiable health information inmates without authorization. Therefore, we add a new provision (§ 164.512(k)(5)) that permits a covered entity to disclose protected health information about inmates without individual consent, authorization, or agreement to correctional institutions for specified health care and other custodial purposes. For example, covered entities are permitted to disclose for the purposes of providing health care to the individual who is the inmate, or for the health and safety of other inmates or officials and employees of the facility. In addition, a covered entity may disclose protected health information as necessary for the administration and maintenance of the safety, security, and good order of the institution. See the preamble discussion of the specific requirements at § 164.512(k)(5), as well as discussion of certain limitations on the rights of individuals who are inmates with regard to their protected health information at §§ 164.506, 164.520, 164.524, and 164.528.

We also provide the following clarifications. Covered entities that provide services to inmates under contract to correctional institutions must treat protected health information about inmates in accordance with this rule and are permitted to use and disclose such information to correctional institutions as allowed under § 164.512(k)(5).

As to former inmates, the final rule considers such persons who are released on parole, probation, supervised release, or are otherwise no longer in custody, to be individuals who are not inmates. Therefore, the permissible disclosure provision at § 164.512(k)(5) does not apply in such cases. Instead, a covered entity must apply privacy protections to the protected health information about former inmates in the same manner and to the same extent that it protects the protected health information of other individuals. In addition, individuals who are former inmates hold the same rights as all other individuals under the rule.

As to individuals in community custody, the final rule considers inmates to be those individuals who are incarcerated in or otherwise confined to a correctional institution. Thus, to the extent that community custody confines an individual to a particular facility, § 164.512(k)(5) is applicable.

Psychotherapy Notes

Comment: Some commenters thought the definition of psychotherapy notes was contrary to standard practice. They claimed that reports of psychotherapy are typically part of the medical record and that psychologists are advised, for ethical reasons and liability risk management purposes, not to keep two separate sets of notes. Others acknowledged that therapists may maintain separate notations of therapy sessions for their own purpose. These commenters asked that we make clear that psychotherapy notes, at least in summary form, should be included in the medical record. Many plans and providers expressed concern that the proposed definition would encourage the creation of ''shadow'' records which may be dangerous to the patient and may increase liability for the health care providers. Some commenters claimed that psychotherapy notes contain information that is often essential to treatment.

Response: We conducted fact-finding with providers and other knowledgeable parties to determine the standard practice of psychotherapists and determined that only some psychotherapists keep separate files with notes pertaining to psychotherapy sessions. These notes are often referred to as ''process notes,'' distinguishable from ''progress notes,'' ''the medical record,'' or ''official records.'' These process notes capture the therapist's

impressions about the patient, contain details of the psychotherapy conversation considered to be inappropriate for the medical record, and are used by the provider for future sessions. We were told that process notes are often kept separate to limit access, even in an electronic record system, because they contain sensitive information relevant to no one other than the treating provider. These separate ''process notes'' are what we are calling ''psychotherapy notes.'' Summary information, such as the current state of the patient, symptoms, summary of the theme of the psychotherapy session, diagnoses, medications prescribed, side effects, and any other information necessary for treatment or payment, is always placed in the patient's medical record. Information from the medical record is routinely sent to insurers for payment.

Comment: Various associations and their constituents asked that the exceptions for psychotherapy notes be extended to health care information from other health care providers. These commenters argued that psychotherapists are not the only providers or even the most likely providers to discuss sensitive and potentially embarrassing issues, as treatment and counseling for mental health conditions, drug abuse, HIV/AIDS, and sexual problems are often provided outside of the traditional psychiatric settings. One writer stated, ''A prudent health care provider will always assess the past and present psychiatric medical history and symptoms of a patient.''

Many commenters believed that the psychotherapy notes should include frequencies of treatment, results of clinical tests, and summary of diagnosis, functional status, the treatment plan, symptoms, prognosis and progress to date. They claimed that this information is highly sensitive and should not be released without the individual's written consent, except in cases of emergency. One commenter suggested listing the types of mental health information that can be requested by third party payors to make payment determinations and defining the meaning of each term.

Response: As discussed above and in the NPRM, the rationale for providing special protection for psychotherapy notes is not only that they contain particularly sensitive information, but also that they are the personal notes of the therapist, intended to help him or her recall the therapy discussion and are of little or no use to others not involved in the therapy. Information in these notes is not intended to communicate to, or even be seen by, persons other than the therapist. Although all psychotherapy information may be considered sensitive, we have limited the definition of psychotherapy notes to only that information that is kept separate by the provider for his or her own purposes. It does not refer to the medical record and other sources of information that would normally be disclosed for treatment, payment, and health care operations.

Comment: One commenter was particularly concerned that the use of the term ''counseling'' in the definition of psychotherapy notes would lead to confusion because counseling and psychotherapy are different disciplines.

Response: In the final rule, we continue to use the term ''counseling'' in the definition of ''psychotherapy.'' During our fact-finding, we learned that ''counseling'' had no commonly agreed upon definition, but seemed to be widely understood in practice. We do not intend to limit the practice of psychotherapy to any specific professional disciplines.

Comment: One commenter noted that the public mental health system is increasingly being called upon to integrate and coordinate services among other providers of mental health services and they have developed an integrated electronic medical record system for state-operated hospitals, part of which includes psychotherapy notes, and which cannot be easily modified to provide different levels of confidentiality. Another commenter recommended allowing use or disclosure of psychotherapy notes by members of an integrated health care facility as well as the originator.

Response: The final rule makes it clear that any notes that are routinely shared with others, whether as part of the medical record or otherwise, are, by definition, not psychotherapy notes, as we have defined them. To qualify for the definition and the increased protection, the notes must be created and maintained for the use of the provider who created them i.e., the originator, and must not be the only source of any information that would be critical for the treatment of the patient or for getting payment for the treatment. The types of notes described in the comment would not meet our definition for psychotherapy notes.

Comment: Many providers expressed concern that if psychotherapy notes were maintained separately from other protected health information, other health providers involved in the individual's care would be unable to treat the patient properly. Some recommended that if the patient does not consent to sharing of psychotherapy notes for treatment purposes, the treating provider should be allowed to decline to treat the patient, providing a referral to another provider.

Response: The final rule retains the policy that psychotherapy notes be separated from the remainder of the medical record in order to receive additional protection. We based this decision on conversations with mental health providers who have told us that information that is critical to the treatment of individuals is normally maintained in the medical record and that psychotherapy notes are used by the provider who created them and rarely for other purposes. A strong part of the rationale for the special treatment of psychotherapy notes is that they are the personal notes of the treating provider and are of little or no use to others who were not present at the session to which the notes refer.

Comment: Several commenters requested that we clarify that the information contained in psychotherapy notes is being protected under the rule and not the notes themselves. They were concerned that the protection for psychotherapy notes would not be meaningful if health plans could demand the same information in a different format.

Response: This rule provides special protection for the information in psychotherapy notes, but it does not extend that protection to the same information that may be found in other locations. We do not require the notes to be in a particular format, such as hand-written. They may be typed into a word processor, for example. Copying the notes into a different format, per se, would not allow the information to be accessed by a health plan. However, the requirement that psychotherapy notes be kept separate from the medical record and solely for the use of the provider who created them means that the special protection does not apply to the same information in another location.

Public Health Authority

Comment: A number of the comments called for the elimination of all permissible disclosures without authorization, and some specifically cited the public health section and its liberal definition of public health authority as an inappropriately broad loophole that would allow unfettered access to private medical information by various government authorities.

Other commenters generally supported the provision allowing disclosure to public health authorities and to non-governmental entities

authorized by law to carry out public health activities. They further supported the broad definition of public health authority and the reliance on broad legal or regulatory authority by public health entities although explicit authorities were preferable and better informed the public.

Response: In response to comments arguing that the provision is too broad, we note that section 1178(b) of the Act, as explained in the NPRM, explicitly carves out protection for state public health laws. This provision states that: ''[N]othing in this part shall be construed to invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth or death, public health surveillance, or public health investigation or intervention.'' In light of this broad Congressional mandate not to interfere with current public health practices, we believe the broad definition of ''public health authority'' is appropriate to achieve that end.

Comment: Some commenters said that they performed public health activities in analyzing data and information. These comments suggested that activities conducted by provider and health plan organizations that compile and compare data for benchmarking performance, monitoring, utilization, and determining the health needs of a given market should be included as part of the public health exemption. One commenter recommended amending the regulation to permit covered entities to disclose protected health information to private organizations for public health reasons.

Response: We disagree that such a change should be made. In the absence of some nexus to a government public health authority or other underlying legal authority, covered entities would have no basis for determining which data collections are ''legitimate'' and how the confidentiality of the information will be protected. In addition, the public health functions carved out for special protection by Congress are explicitly limited to those established by law.

Comment: Two commenters asked for additional clarification as to whether the Occupational Safety and Health Administration (OSHA) and the Mine Safety and Health Administration (MSHA) would be considered public health authorities as indicated in the preamble. They suggested specific language for the final rule. Commenters also suggested that we specify that states operating OSHA-approved programs also are considered public health authorities. One comment applauded the Secretary's recognition of OSHA as both a health oversight agency and public health authority. It suggested adding OSHA-approved programs that operate in states to the list of entities included in these categories. In addition, the comment requested the final regulation specifically mention these entities in the text of the regulation as well.

Response: We agree that OSHA, MSHA and their state equivalents are public health authorities when carrying out their activities related to the health and safety of workers. We do not specifically reference any agencies in the regulatory definition, because the definition of public health authority and this preamble sufficiently address this issue. As defined in the final rule, the definition of ''public health authority'' at § 164.501 continues to include OSHA as a public health authority. State agencies or authorities responsible for public health matters as part of their official mandate, such as OSHA-approved programs, also come within this definition. See discussion of § 164.512(b) below. We have refrained, however, from listing specific agencies and have retained a general descriptive definition.

Comments: Several commenters recommended expanding the definition of public health authority to encompass other governmental entities that may collect and hold health data as part of their official duties. One recommended changing the definition of public health authority to read as follows: Public health authority means an agency or authority * * * that is responsible for public health matters or the collection of health data as part of its official mandate.

Response: We do not adopt this recommendation. The public health provision is not intended to cover agencies that are not responsible for public health matters but that may in the course of their responsibilities collect health-related information. Disclosures to such authorities may be permissible under other provision of this rule.

Comment: Many commenters asked us to include a formal definition of ''required by law'' incorporating the material noted in this preamble and additional suggested disclosures.

Response: We agree generally and modify the definition accordingly. See discussion above.

Research

Comment: We received many comments from supporting the proposed definition of ''research.'' These commenters agreed that the definition of ''research'' should be the same as the definition in the Common Rule. These commenters argued that it was important that the definition of ''research'' be consistent with the Common Rule's definition to ensure the coherent oversight of medical research. In addition, some of these commenters also supported this definition because they believed it was already well-understood by researchers and provided reasonably clear guidance needed to distinguish between research and health care operations.

Some commenters, believed that the NPRM's definition was too narrow. Several of these commenters agreed that the Common Rule's definition should be adopted in the final rule, but argued that the proposed definition of ''generalizable knowledge'' within the definition of ''research,'' which limited generalizable knowledge to knowledge that is ''related to health,'' was too narrow. For example, one commenter stated that gun shot wound, spousal abuse, and other kinds of information from emergency room statistics are often used to conduct research with ramifications for social policy, but may not be ''related to health.'' Several of these commenters recommended that the definition of research be revised to delete the words ''related to health.'' Additional commenters who argued that the definition was too narrow raised the following concerns: the difference between ''research'' and ''health care operations'' is irrelevant from the patients' perspective, and therefore, the proposed rule should have required documentation of approval by an IRB or privacy board before protected health information could be used or disclosed for either of these purposes, and the proposed definition was too limited because it did not capture research conducted by non-profit entities to ensure public health goals, such as disease-specific registries.

Commenters who argued that the definition was too broad recommended that certain activities should be explicitly excluded from the definition. In general, these commenters were concerned that if certain activities were considered to be ''research'' the rule's research requirements would represent a problematic level of regulation on industry initiatives. Some activities that these commenters recommended be explicitly excluded from the definition of ''research'' included: marketing research, health and productivity management, quality assessment and improvement activities, and internal research conducted to improve health.

Response: We agree that the final rule's definition of ''research'' should be

consistent with the Common Rule's definition of this term. We also agree that our proposal to limit ''generalizable knowledge'' to knowledge that is ''related to health,'' and ''knowledge that could be applied to populations outside of the population served by the covered entity,'' was too narrow. Therefore, in the final rule, we retain the Common Rule's definition of ''research'' and eliminate the further elaboration of ''generalizable knowledge.'' We understand knowledge to be generalizable when it can be applied to either a population inside or outside of the population served by the covered entity. Therefore, knowledge may be ''generalizable'' even if a research study uses only the protected health information held within a covered entity, and the results are generalizable only to the population served by the covered entity. For example, generalizable knowledge could be generated from a study conducted by the HCFA, using only Medicare data held by HCFA, even if the knowledge gained from the research study is applicable only to Medicare beneficiaries.

We rejected the other arguments claiming that the definition of ''research'' was either too narrow or too broad. While we agree that it is sometimes difficult to distinguish between ''research'' and ''health care operations,'' we disagree that the difference between these activities is irrelevant from the patients' perspective. We believe, based on many of the comments, that individuals expect that individually identifiable health information about themselves will be used for health care operations such as reviewing the competence or qualifications of health care professionals, evaluating provider and plan performance, and improving the quality of care. A large number of commenters, however, indicated that they did not expect that individually identifiable health information about themselves would be used for research purposes without their authorization. Therefore, we retain more stringent protections for research disclosures without patient authorization.

We also disagree with the commenters who were concerned that the proposed definition was too limited because it did not capture research conducted by non-profit entities to ensure public health goals, such as disease-specific registries. Such activities conducted by either non-profit or for-profit entities could meet the rule's definition of research, and therefore are not necessarily excluded from this definition.

We also disagree with many of the commenters who argued that certain activities should be explicitly excluded from the definition of research. We found no persuasive evidence that, when particular activities are also systematic investigations designed to contribute to generalizable knowledge, they should be treated any different from other such activities.

We are aware that the National Bioethics Advisory Commission (NBAC) is currently assessing the Common Rule's definition of ''research'' as part of a report they are developing on the implementation and adequacy of the Common Rule. Since we agree that a consistent definition is important to the conduct and oversight of research, if the Common Rule's definition of ''research'' is modified in the future, the Department of Health and Human Services will consider whether the definition should also be modified for this subpart.

Comment: Some commenters urged the Department to establish precise definitions for ''health care operations'' and ''research'' to provide clear guidance to covered entities and adequate privacy protections for the subjects of the information whose information is disclosed for these purposes. One commenter supported the definition of ''research'' proposed in the NPRM, but was concerned about the ''crossover'' from data analyses that begin as health care operations but later become ''research'' because the analytical results are of such importance that they should be shared through publication, thereby contributing to generalizable knowledge. To distinguish between the definitions of ''health care operations'' and ''research,'' a few commenters recommended that the rule make this distinction based upon whether the activity is a ''use'' or a ''disclosure.'' These commenters recommend that the ''use'' of protected health information for research without patient authorization should be exempt from the proposed research provisions provided that protected health information was not disclosed in the final analysis, report, or publication.

Response: We agree with commenters that at times it may be difficult to distinguish projects that are health operations and projects that are research. We note that this ambiguity exists today, and disagree that we can address this issue with more precise definitions of research and health care operations. Today, the issue is largely one of intent. Under the Common Rule, the ethical and regulatory obligations of the researcher stem from the intent of the activity. We follow that approach here. If such a project is a systematic investigation that designed to develop or contribute to generalizable knowledge, it is considered to be ''research,'' not ''health care operations.''

In some instances, the primary purpose of the activity may change as preliminary results are analyzed. An activity that was initiated as an internal outcomes evaluation may produce information that could be generalized. If the purpose of a study changes and the covered entity does intend to generalize the results, the covered entity should document the fact as evidence that the activity was not subject to § 164.512(i) of this rule.

We understand that for research that is subject to the Common Rule, this is not the case. The Office for Human Research Protection interprets 45 CFR part 46 to require IRB review as soon as an activity meets the definition of research, regardless of whether the activity began as ''health care operations'' or ''public health,'' for example. The final rule does not affect the Office of Human Research Protection's interpretation of the Common Rule.

We were not persuaded that an individual's privacy interest is of less concern when covered entities use protected health information for research purposes than when covered entities disclose protected health information for research purposes. We do not agree generally that internal activities of covered entities do not potentially compromise the privacy interests of individuals. Many persons within a covered entity may have access to protected health information. When the activity is a systematic investigation, the number of persons who may be involved in the records review and analysis may be substantial. We believe that IRB or privacy board approval of the waiver of authorization will provide important privacy protections to individuals about whom protected health information is used or disclosed for research. If a covered entity wishes to use protected health information about its enrollees for research purposes, documentation of an IRBs' or privacy board's assessment of the privacy impact of such a use is as important as if the same research study required the disclosure of protected health information. This conclusion is consistent with the Common Rule's requirement for IRB review of all human subjects research.

Treatment

Comment: Some commenters advocated for a narrow interpretation of

treatment that applies only to the individual who is the subject of the information. Other commenters asserted that treatment should be broadly defined when activities are conducted by health care providers to improve or maintain the health of the patient. A broad interpretation may raise concerns about potential misuse of information, but too limited an interpretation will limit beneficial activities and further contribute to problems in patient compliance and medical errors.

Response: We find the commenters' arguments for a broad definition of treatment persuasive. Today, health care providers consult with one another, share information about their experience with particular therapies, seek advice about how to handle unique or challenging cases, and engage in a variety of other discussions that help them maintain and improve the quality of care they provide. Quality of care improves when providers exchange information about treatment successes and failures. These activities require sharing of protected health information. We do not intend this rule to interfere with these important activities. We therefore define treatment broadly and allow use and disclosure of protected health information about one individual for the treatment of another individual.

Under this definition, only health care providers or a health care provider working with a third party can perform treatment activities. In this way, we temper the breadth of the definition by limiting the scope of information sharing. The various codes of professional ethics also help assure that information sharing among providers for treatment purposes will be appropriate.

We note that poison control centers are health care providers for purposes of this rule. We consider the counseling and follow-up consultations provided by poison control centers with individual providers regarding patient outcomes to be treatment. Therefore, poison control centers and other health care providers can share protected health information about the treatment of an individual without a business associate contract.

Comment: Many commenters suggested that ''treatment'' activities should include services provided to both a specific individual and larger patient populations and therefore urged that the definition of treatment specifically allow for such activities, sometimes referred to as ''disease management'' activities. Some argued that an analysis of an overall population is integral to determining which individuals would benefit from disease management services. Thus, an analysis of health care claims for enrolled populations enables proactive contact with those identified individuals to notify them of the availability of services. Certain commenters noted that ''disease management'' services provided to their patient populations, such as reminders about recommended tests based on nationally accepted clinical guidelines, are integral components of quality health care.

Response: We do not agree that population based services should be considered treatment activities. The definition of ''treatment'' is closely linked to the § 160.103 definition of ''health care,'' which describes care, services and procedures related to the health of an individual. The activities described by ''treatment,'' therefore, all involve health care providers supplying health care to a particular patient. While many activities beneficial to patients are offered to entire populations or involve examining health information about entire populations, treatment involves health services provided by a health care provider and tailored to the specific needs of an individual patient. Although a population-wide analysis or intervention may prompt a health care provider to offer specific treatment to an individual, we consider the population-based analyses to improve health care or reduce health care costs to be health care operations (see definition of ''health care operations,'' above).

Comment: A number of commenters requested clarification about whether prescription drug compliance management programs would be considered ''treatment.'' One commenter urged HHS to clarify that provision by a pharmacy to a patient of customized prescription drug information about the risks, benefits, and conditions of use of a prescription drug being dispensed is considered a treatment activity. Others asked that the final rule expressly recognize that prescription drug advice provided by a dispensing pharmacist, such as a customized pharmacy letter, is within the scope of treatment.

Response: The activities that are part of prescription drug compliance management programs were not fully described by these commenters, so we cannot state a general rule regarding whether such activities constitute treatment. We agree that pharmacists' provision of customized prescription drug information and advice about the prescription drug being dispensed is a treatment activity. Pharmacists' provisions of information and counseling about pharmaceuticals to their customers constitute treatment, and we exclude certain communications made in the treatment context from the definition of marketing. (See discussion above.)

Comment: Some commenters noted the issues and recommendations raised in the Institutes of Medicine report ''To Err Is Human'' and the critical need to share information about adverse drug and other medical events, evaluation of the information, and its use to prevent future medical errors. They noted that privacy rules should not be so stringent as to prohibit the sharing of patient data needed to reduce errors and optimize health care outcomes. To bolster the notion that other programs associated with the practice of pharmacy must be considered as integral to the definition of health care and treatment, they reference OBRA '90 (42 U.S.C. 1396r–8) and the minimum required activities for dispensing drugs; they also note that virtually every state Board of Pharmacy adopted regulations imposing OBRA'90 requirements on pharmacies for all patients and not just Medicaid recipients.

Response: We agree that reducing medical errors is critical, and do not believe that this regulation impairs efforts to reduce medical errors. We define treatment broadly and include quality assessment and improvement activities in the definition of health care operations. Covered pharmacies may conduct such activities, as well as treatment activities appropriate to improve quality and reduce errors. We believe that respect for the privacy rights of individuals and appropriate protection of the confidentiality of their health information are compatible with the goal of reducing medical errors.

Comment: Some commenters urged us to clarify that health plans do not perform ''treatment'' activities; some of these were concerned that a different approach in this regulation could cause conflict with state corporate practice of medicine restrictions. Some commenters believed that the proposed definition of treatment crossed into the area of cost containment, which would seem to pertain more directly to payment. They supported a narrower definition that would eliminate any references to third party payors. One commenter argued that the permissible disclosure of protected health information to carry out treatment is too broad for health plans and that health plans that have no responsibility for treatment or care coordination should have no authority to release health information without authorization for treatment purposes.

Response: We do not consider the activities of third party payors, including health plans, to be

''treatment.'' Only health care providers, not health plans, conduct ''treatment'' for purposes of this rule. A health plan may, however, disclose protected health information without consent or authorization for treatment purposes if that disclosure is made to a provider. Health plans may have information the provider needs, for example information from other providers or information about the patient's treatment history, to develop an appropriate plan of care.

Comment: We received many comments relating to ''disease management'' programs and whether activities described as disease management should be included in the definition of treatment. One group of commenters supported the proposed definition of treatment that includes disease management. One commenter offered the position that disease management services are more closely aligned with treatment because they involve the coordination of treatment whereas health care operations are more akin to financial and ministerial functions of plans.

Some recommended that the definition of treatment be limited to direct treatment of individual patients and not allow for sharing of information for administrative or other programmatic reasons. They believed that allowing disclosures for disease management opens a loophole for certain uses and disclosures, such as marketing, that should only be permitted with authorization. Others recommended that the definition of disease management be restricted to prevent unauthorized use of individual health records to target individuals in a health plan or occupational health program. Many asked that the definition of disease management be clarified to identify those functions that, although some might consider them to be subsumed by the term, are not permitted under this regulation without authorization, such as marketing and disclosures of protected health information to employers. They suggested that disease management may describe desirable activities, but is subject to abuse and therefore should be restricted and controlled. One commenter recommends that we adopt a portion of the definition adopted by the Disease Management Association of America in October 1999.

On the other hand, many comments urged that disease management be part of the ''treatment'' definition or the ''health care operations'' definition and asked that specific activities be included in a description of the term. They viewed disease management as important element of comprehensive health care services and cost management efforts. They recommended that the definition of disease management include services directed at an entire population and not just individual care, in order to identify individuals who would benefit from services based on accepted clinical guidelines. They recommended that disease management be included under health care operations and include population level services. A commenter asserted that limiting disease management programs to the definition of treatment ignores that these programs extend beyond providers, especially since NCQA accreditation standards strongly encourage plans and insurers to provide these services.

Response: Disease management appeared to represent different activities to different commenters. Our review of the literature, industry materials, state and federal statutes,[6] and discussions with physician groups, health plan groups and disease management associations confirm that a consensus definition from the field has not yet evolved, although efforts are underway. Therefore, rather than rely on this label, we delete ''disease management'' from the treatment definition and instead include the functions often discussed as disease management activities in this definition or in the definition of health care operations and modify both definitions to address the commenters' concerns.

We add population-based activities to improve health care or reduce health care costs to the definition of health care operations. Outreach programs as described by the commenter may be considered either health care operations or treatment, depending on whether population-wide or patient-specific activities occur, and if patient-specific, whether the individualized communication with a patient occurs on behalf of health care provider or a health plan. For example, a call placed by a nurse in a doctor's office to a patient to discuss follow-up care is a treatment activity. The same activity performed by a nurse working for a health plan would be a health care operation. In both cases, the database analysis that created a list of patients that would benefit from the intervention would be a health care operation. Use or disclosure of protected health information to provide education materials to patients may similarly be either treatment or operations, depending on the circumstances and on who is sending the materials. We cannot say in the abstract whether any such activities constitute marketing under this rule. See §§ 164.501 and 164.514 for details on what communications are marketing and when the authorization of the individual may be required.

Comment: Many commenters were concerned that the definition of treatment would not permit Third Party Administrators (TPAs) to be involved with disease management programs without obtaining authorization. They asserted that while the proposed definition of treatment included disease management conducted by health care providers it did not recognize the role of employers and TPAs in the current disease management process.

Response: Covered entities disclose protected health information to other persons, including TPAs, that they hire to perform services for them or on their behalf. If a covered entity hires a TPA to perform the disease management activities included in the rule's definitions of treatment and health care operations that disclosure will not

[6] Definition of Disease Management, October 1999 (from web site of Disease Management Association of America (www.dmaa.org/definition.html) accessed May 21, 2000. Other references used for our analysis include: Mary C. Gurnee, et al, Constructing Disease Management Programs, Managed Care, June 1997, accessed at http://managedcaremag.com, 5/19/2000; Peter Wehrwein, Disease Management Gains a Degree of Respectability, Managed Care, August 1997, accessed at www.managedcaremag.com, 5/18/00; John M. Harris, Jr., disease management: New Wine in Old Bottles, 124 Annals of Internal Medicine 838 (1996); Robert S. Epstein and Louis M. Sherwood, From Outcomes research to disease management: A Guide for the Perplexed, 124 Annals of Internal Medicine 832 (1996); Anne Mason et al, disease management, the Pharmaceutical Industry and the NHS, Office of Health Economics (United Kingdom), accessed at www.ohe.org, 5/19/2000; Thomas Bodenheimer, Disease Management—Promises and Pitfalls, 340 New Eng. J. Med, April 15, 1999, accessed at www.nejm.org, 4/20/99; Bernard Lo and Ann Alpers, Uses and Abuses of Prescription Drug information in pharmacy benefits Management Programs, 283 JAMA 801 (2000); Robert F. DeBusk, Correspondence, Disease Management, and Regina E. Herzlinger, Correspondence, Disease Management, 341 New Eng. J. Med, Sept 2, 1999, accessed 9/2/99; Letter, John A. Gans, American Pharmaceutical Association, to Health Care Financing Administration, Reference HCFA–3002–P, April 12, 1999, accessed at www.aphanet.org, 1/18/2000; Ronald M. Davis, et al, Editorial, Advances in Managing Chronic Disease, 320 BMJ 525 (2000), accessed at www.bmj.com, 2/25/00; Thomas Bodenheimer, Education and Debate, disease management in the American Market, 320 BMJ 563 (2000), accessed at www.bmj.com, 2/25/2000; David J. Hunter, disease management: has it a future?, 320 BMJ 530 (2000), accessed www.bmj.com 2/25/2000; Trisha Greenhalgh, Commercial partnerships in chronic disease management: proceeding with caution, 320 BMJ 566 (2000); Edmund X. DeJesus, disease management in a Warehouse, Healthcare Informatics, September 1999, accessed at www.healthcare-informatics.com, 5/19/00; Regulation, 42 CFR 422.112, Medicare+Choice Program, subpart C, Benefits and Beneficiary Protections, sec. 422.112, Access to Services; and Arnold Chen, Best Practices in Coordinated Care, Submitted by Mathematica Policy Research, Inc., to Health Care Financing Administration, March 22, 2000.

require authorization. The relationship between the covered entity and the TPA may be subject to the business associate requirements of §§ 164.502 and 164.504. Disclosures by covered entities to plan sponsors, including employers, for the purpose of plan administration are addressed in § 164.504.

Comment: Commenters suggested that as disease management is defined only as an element of treatment, it could only be carried out by health care providers, and not health plans. They opposed this approach because health plans also conduct such programs, and are indeed required to do it by accreditation standards and HCFA Managed Care Organization standards.

Response: We agree that the placement of disease management in the proposed definition of treatment suggested that health plans could not conduct such programs. We revise the final rule to clarify that health plans may conduct population based care management programs as a health care operation activity.

Comment: Some commenters stated that the rule should require that disease management only be done with the approval of the treating physician or at least with the knowledge of the physician.

Response: We disagree with this comment because we do not believe that this privacy rule is an appropriate venue for setting policies regarding the management of health care costs or treatment.

Comment: Some industry groups stated that if an activity involves selling products, it is not disease management. They asked for a definition 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 eliminate the definition of ''disease management'' from the rule. Often however, treatment decisions involve discussing the relevant advantages and disadvantages of products and services. Health plans, as part of payment and operations, sometimes communicate with individuals about particular products and services. We address these distinctions in the definitions of marketing and ''health care operations'' in § 164.501, and in the requirements for use and disclosure of protected health information for marketing in § 164.514.

Comment: Some health care providers noted that there is a danger that employers will ''force'' individual employees with targeted conditions into self-care or compliance programs in ways that violate both the employee's privacy interest and his or her right to control own medical care.

Response: Employers are not covered entities under HIPAA, so we cannot prohibit them under this rule from undertaking these or other activities with respect to health information. In § 164.504 we limit disclosure of health information from group health plans to the employers sponsoring the plans. However, other federal and/or state laws, such as disability nondiscrimination laws, may govern the rights of employees under such circumstances.

Comment: Many commenters urged that disease management only be allowed with the written consent of the individual. Others also desired consent but suggested that an opt-out would be sufficient. Other 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 were concerned 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.

Response: We agree with the commenters who stated that the requirement for specific authorization for certain activities considered part of disease management could impede the ability of health plans and covered providers to implement effective health care management and cost containment programs. In addition, this approach would require us to distinguish activities undertaken as part of a formal disease management program from the same activities undertaken outside the context of disease management program. For example, we see no clear benefit to privacy in requiring written authorization before a physician may call a patient to discuss treatment options in all cases, nor do we see a sound basis for requiring it only when the physician was following a formal protocol as part of a population based intervention. We also are not persuaded that the risk to privacy for these activities warrants a higher degree of protection than do other payment, health care operations or treatment activities for which specific authorization was not suggested by commenters.

Comment: A few commenters asked that we clarify that disclosure of protected health information about a prospective patient to a health care provider (e.g., a possible admission to an assisted living facility from a nursing facility) is a treatment activity that does not require authorization.

Response: We agree that the described activity is ''treatment,'' because it constitutes referral and coordination of health care.

Comment: Comments called for the removal of ''other services'' from the definition.

Response: We disagree with the concept that only health care services are appropriately included in the treatment definition. We have modified this definition to instead include ''the provision, coordination, or management of health care and related services.'' This definition allows health care providers to offer or coordinate social, rehabilitative, or other services that are associated with the provision of health care. Our use of the term ''related'' prevents ''treatment'' from applying to the provision of services unrelated to health care.

Comment: Several commenters stated that the definition of treatment should include organ and tissue recovery activities. They asserted that the information exchanged and collected to request consent, evaluate medical information about a potential donor and perform organ recoveries relates to treatment and are not administrative activities. When hospitals place a patient on the UNOS list it is transferring individually identifiable health information. Also, when an organ procurement organization registers a donor with UNOS it could be disclosing protected health information. Commenters questioned whether these activities would be administrative or constitute treatment.

Response: In the proposed rule we included in the definition of ''health care'' activities related to the procurement or organs, blood, eyes and other tissues. This final rule deletes those activities from the definition of ''health care.'' We do so because, while organ and tissue procurement organizations are integral components of the health care system, we do not believe that the testing, procurement, and other procedures they undertake describe ''health care'' offered to the donors of the tissues or organs themselves. See the discussion under the definition of ''health care'' in § 160.103.

Comment: Some commenters recommended including health promotion activities in the definition of health care.

Response: We consider health promotion activities to be preventive care, and thus within the definition of health care. In addition, such activities that are population based are included in the definition of health care operations.

Comment: We received a range of comments regarding the proper placement of case and disease management in the definitions and the perceived overlap between health care operations and treatment. Some consider that these activities are a function of improving quality and controlling costs. Thus, they recommend that the Secretary move risk assessment, case and disease management to the definition of health care operations.

Response: In response to these comments, we remove these terms from the definition of treatment and add case management to the definition of health care operations. We explain our treatment of disease management in responses to comments above. Whether an activity described as disease or case management falls under treatment or health care operations would depend in part on whether the activity is focused on a particular individual or a population. A single program described as a ''case management'' effort may include both health care operations activities (e.g., records analysis, protocol development, general risk assessment) and treatment activities (e.g., particular services provided to or coordinated for an individual, even if applying a standardized treatment protocol).

Comment: We received comments that argued for the inclusion of ''disability management'' in the treatment definition. They explained that through disability management, health care providers refer and coordinate medical management and they require contemporaneous exchange of an employee's specific medical data for the provider to properly manage.

Response: To the extent that a covered provider is coordinating health care services, the provider is providing treatment. We do not include the term ''disability management'' because the scope of the activities covered by that term is not clear. In addition, the commenters did not provide enough information for us to make a fact-based determination of how this rule applies to the uses and disclosures of protected health information that are made in a particular ''disability management'' program.

Use

Comment: One commenter asserted that the scope of the proposal had gone beyond the intent of Congress in addressing uses of information within the covered entity, as opposed to transactions and disclosures outside the covered entity. This commenter argued that, although HIPAA mentions use, it is unclear that the word ''use'' in the proposed rule is what Congress intended. The commenter pointed to the legislative history to argue that ''use'' is related to an information exchange outside of the entity.

Response: We disagree with the commenter regarding the Congress' intent. Section 264 of HIPAA requires that the Secretary develop and send to Congress recommendations on standards with respect to the privacy of individually identifiable health information (which she did on September 11, 1997) and prescribes that the recommendations address among other items ''the uses and disclosures of such information that should be authorized or required.'' Section 264 explicitly requires the Secretary to promulgate standards that address at least the subjects described in these recommendations. It is therefore our interpretation that Congress intended to cover ''uses'' as well as disclosures of individually identifiable health information. We find nothing in the legislative history to indicate that Congress intended to deviate from the common meaning of the term ''use.''

Comment: One commenter observed that the definition could encompass the processing of data by computers to execute queries. It was argued that this would be highly problematic because computers are routinely used to identify subsets of data sets. It was explained that in performing this function, computers examine each record in the data set and return only those records in the data set that meet specific criteria. Consequently, a human being will see only the subset of data that the computer returns. Thus, the commenter stated that it is only this subset that could be used or disclosed.

Response: We interpret ''use'' to mean only the uses of the product of the computer processing, not the internal computer processing that generates the product.

Comments: Some commenters asked that the Department clarify that individualized medical information obtained through a fitness for duty examination is not subject to the privacy protections under the regulation.

Response: As discussed above, we have clarified that the definition of ''treatment'' to include assessments of an individual. If the assessment is performed by a covered health care provider, the health information resulting from the assessment is protected health information. We note that a covered entity is permitted to condition the provision of health care when the sole purpose is to create protected health information for the benefit of a third person. See § 164.508(b). For example, a covered health care provider may condition the provision of a fitness for duty examination to an individual on obtaining an authorization from the individual for disclosure to the employer who has requested the examination.

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

Section 164.502(a)—General Standard

Comment: A few commenters requested an exemption from the rule for the Social Security and Supplemental Security Income Disability Programs so that disability claimants can be served in a fair and timely manner. The commenters were concerned that the proposal would be narrowly interpreted, thereby impeding the release of medical records for the purposes of Social Security disability programs.

Another commenter similarly asked that a special provision be added to the proposal's general rule for uses and disclosures without authorization for treatment, payment, and health care operations purposes to authorize disclosure of all medical information from all sources to the Social Security Administration, including their contracted state agencies handling disability determinations.

Response: A complete exemption for disclosures for these programs is not necessary. Under current practice, the Social Security Administration obtains authorization from applicants for providers to release an individual's records to SSA for disability and other determinations. Thus, there is no reason to believe that an exemption from the authorization required by this rule is needed to allow these programs to function effectively. Further, such an exemption would reduce privacy protections from current levels. When this rule goes into effect, those authorizations will need to meet the requirements for authorization under § 164.508 of this rule.

We do, however, modify other provisions of the proposed rule to accommodate the special requirements of these programs. In particular, Social Security Disability and other federal programs, and public benefits programs run by the states, are authorized by law

to share information for eligibility purposes. Where another public body has determined that the appropriate balance between need for efficient administration of public programs and public funds and individuals' privacy interests is to allow information sharing for these limited purposes, we do not upset that determination. Where the sharing of enrollment and eligibility information is required or expressly authorized by law, this rule permits such sharing of information for eligibility and enrollment purposes (see § 164.512(k)(6)(i)), and also excepts these arrangements from the requirements for business associate agreements (see § 164.502(e)(1)).

Comment: A few commenters asked that the rule be revised to authorize disclosures to clergy, for directory purposes, to organ and tissue procurement organizations, and to the American Red Cross without patient authorization.

Response: We agree and revise the final rule accordingly. The new policies and the rationale for these policies are found in §§ 164.510 and 164.512, and the corresponding preamble.

Comment: One commenter recommended that the rule apply only to the ''disclosure'' of protected health information by covered entities, rather than to both ''use'' and ''disclosure.'' The commenter stated that the application of the regulation to a covered entity's use of individually identifiable health information offers little benefit in terms of protecting protected health information, yet imposes costs and may hamper many legitimate activities, that fall outside the definition of treatment, payment or health care operations.

Another commenter similarly urged that the final regulation draw substantive distinctions between restrictions on the ''use'' of individually identifiable health information and on the ''disclosure'' of such information, with broader latitude for ''uses'' of such information. The commenter believed that internal ''uses'' of such information generally do not raise the same issues and concerns that a disclosure of that information might raise. It was argued that any concerns about the potential breadth of use of this information could be addressed through application of the ''minimum necessary'' standard. The commenter also argued that Congressional intent was that a ''disclosure'' of individually identifiable health information is potentially much more significant than a ''use'' of that information.

Response: We do not accept the commenter's broad recommendation to apply the regulation only to the ''disclosure'' of protected health information and not to ''use'' of such information. Section 264 charges the Secretary with promulgating standards that address, among other things, ''the uses and disclosures'' of individually identifiable health information. We also do not agree that applying the regulation to ''use'' offers little benefit to protecting protected health information. The potential exists for misuse of protected health information within entities. This potential is even greater when the covered entity also provides services or products outside its role as a health care provider, health plan, or health care clearinghouse for which ''use'' of protected health information offers economic benefit to the entity. For example, if this rule did not limit ''uses'' generally to treatment, payment and health care operations, a covered entity that also offered financial services could be able to use protected health information without authorization to market or make coverage or rate decisions for its financial services products. Without the minimum necessary standard for uses, a hospital would not be constrained from allowing their appointment scheduling clerks free access to medical records.

We agree, however, that it is appropriate to apply somewhat different requirements to uses and disclosures of protected health information permitted by this rule. We therefore modify the application of the minimum necessary standard to accomplish this. See the preamble to § 164.514 for a discussion of these changes.

Comment: A commenter argued that the development, implementation, and use of integrated computer-based patient medical record systems, which requires efficient information sharing, will likely be impeded by regulatory restrictions on the ''use'' of protected health information and by the minimum necessary standard.

Response: We have modified the proposed approach to regulating ''uses'' of protected health information within an entity, and believe our policy is compatible with the development and implementation of computer-based medical record systems. In fact, we drew part of the revised policy on ''minimum necessary'' use of protected health information from the role-based access approach used in several computer-based records systems today. These policies are described further in § 164.514.

Comment: One commenter asked that the general rules for uses and disclosures be amended to permit covered entities to disclose protected health information for purposes relating to property and casualty benefits. The commenter argued that the proposal could affect its ability to obtain protected health information from covered entities, thereby constricting the flow of medical information needed to administer property and casualty benefits, particularly in the workers' compensation context. It was stated that this could seriously impede property and casualty benefit providers' ability to conduct business in accordance with state law.

Response: We disagree that the rule should be expanded to permit all uses and disclosures that relate to property and casualty benefits. Such a broad provision is not in keeping with protecting the privacy of individuals. Although we generally lack the authority under HIPAA to regulate the practices of this industry, the final rule addresses when covered entities may disclose protected health information to property and casualty insures. We believe that the final rule permits property and casualty insurers to obtain the protected health information that they need to maintain their promises to their policyholders. For example, the rule permits a covered entity to use or disclose protected health information relating to an individual when authorized by the individual. Property and casualty insurers are free to obtain authorizations from individuals for release by covered entities of the health information that the insurers need to administer claims, and this rule does not affect their ability to condition payment on obtaining such an authorization from insured individuals. Property and casualty insurers providing payment on a third-party basis have an opportunity to obtain authorization from the individual and to condition payment on obtaining such authorization. The final rule also permits covered entities to make disclosures to obtain payment, whether from a health plan or from another person such as a property and casualty insurer. For example, where an automobile insurer is paying for medical benefits on a first-party basis, a health care provider may disclose protected health information to the insurer as part of a request for payment. We also include in the final rule a new provision that permits covered entities to use or disclose protected health information as authorized by workers' compensation or similar programs established by law addressing work-related injuries or illness. See § 164.512(l). These statutory programs establish channels of information sharing that are necessary

to permit compensation of injured workers.

Comment: A few commenters suggested that the Department specify ''prohibited'' uses and disclosures rather than ''permitted'' uses and disclosures.

Response: We reject these commenters' because we believe that the best privacy protection in most instances is to require the individual's authorization for use or disclosure of information, and that the role of this rule is to specify those uses and disclosures for which the balance between the individuals' privacy interest and the public's interests dictates a different approach. The opposite approach would require us to anticipate the much larger set of all possible uses of information that do not implicate the public's interest, rather than to specify the public interests that merit regulatory protection.

Comment: A commenter recommended that the rule be revised to more strongly discourage the use of individually identifiable health information where de-identified information could be used.

Response: We agree that the use of de-identified information wherever possible is good privacy practice. We believe that by requiring covered entities to implement these privacy restrictions only with respect to individually identifiable health information, the final rule strongly encourages covered entities to use de-identified information as much as practicable.

Comment: One commenter recommended that when information from health records is provided to authorized external users, this information should be accompanied by a statement prohibiting use of the information for other than the stated purpose; prohibiting disclosure by the recipient to any other party without written authorization from the patient, or the patient's legal representative, unless such information is urgently needed for the patient's continuing care or otherwise required by law; and requiring destruction of the information after the stated need has been fulfilled.

Response: We agree that restricting other uses or re-disclosure of protected health information by a third party that may receive the information for treatment, payment, and health care operations purposes or other purposes permitted by rule would be ideal with regard to privacy protection. However, as described elsewhere in this preamble, once protected health information leaves a covered entity the Department no longer has jurisdiction under the statute to apply protections to the information. Since we would have no enforcement authority, the costs and burdens of requiring covered entities to produce and distribute such a statement to all recipients of protected heath information, including those with whom the covered entity has no on-going relationship, would outweigh any benefits to be gained from such a policy. Similarly, where protected health information is disclosed for routine treatment, payment and operations purposes, the sheer volume of these disclosures makes the burden of providing such a statement unacceptable. Appropriate protection for these disclosures requires law or regulation directly applicable to the recipient of the information, not further burden on the disclosing entity. Where, however, the recipient of protected health information is providing a service to or on behalf of the covered entity this balance changes. It is consistent with long-standing legal principles to hold the covered entity to a higher degree of responsibility for the actions of its agents and contractors. See § 164.504 for a discussion of the responsibilities of covered entities for the actions of their business associates with respect to protected health information.

Section 164.502(b)—Minimum Necessary

Comments on the minimum necessary standard are addressed in the preamble to § 164.514(d).

Section 164.502(c)—Uses or Disclosures of Protected Health Information Subject to an Agreed Upon Restriction

Comments on the agreed upon restriction standard are addressed in the preamble to § 164.522(a).

Section 164.502(d)—Uses and Disclosures of De-Identified Protected Health Information

Comments on the requirements for de-identifying information are addressed in the preamble to § 164.514(a)–(c).

Section 164.502(e)—Business Associates

Comments on business associates are addressed in the preamble to § 164.504(e).

Section 164.502(f)—Deceased Individuals

Comment: Most commenters on this topic generally did not approve of the Secretary's proposal with regard to protected health information about deceased individuals. The majority of these commenters argued that our proposal was not sufficiently protective of such information. Commenters agreed with the statements made in the preamble to the proposed rule that the privacy concerns addressed by this policy are not limited to the confidential protection of the deceased individual but instead also affects the decedent's family, as genetic information and information pertinent to hereditary diseases and risk factors for surviving relatives and direct family members may be disclosed through the disclosure of the deceased individual's confidential data. It was argued that the proposal would be inadequate to protect the survivors who could be negatively affected and in most cases will outlive the two-year period of protection. A number of medical associations asserted that individuals may avoid genetic testing, diagnoses, and treatment and suppress information important to their health care if they fear family members will suffer discrimination from the release of their medical information after their death. One commenter pointed out that ethically little distinction can be made between protecting an individual's health information during life and protecting it post-mortem. Further, it was argued that the privacy of the deceased individual and his or her family is far more important than allowing genetic information to be abstracted by an institutional or commercial collector of information. A few commenters asked that we provide indefinite protection on the protected health information about a deceased person contained in psychotherapy notes. One commenter asked that we extend protections on records of children who have died of cancer for the lifetime of a deceased child's siblings and parents.

The majority of commenters who supported increased protections on the protected health information about the deceased asked that we extend protections on such information indefinitely or for as long as the covered entity maintains the information. It was also argued that the administrative burden of perpetual protection would be no more burdensome than it is now as current practice is that the confidentiality of identifiable patient information continues after death. A number of others pointed out that there was no reason to set a different privacy standard for deceased individuals than we had for living individuals and that it has been standard practice to release the information of deceased individuals with a valid consent of the executor, next of kin, or specific court order. In addition, commenters referenced Hawaii's health care information privacy law (see Haw. Rev. Stat. section

323C–43) as at least one example of a state law where the privacy and access provisions of the law continue to apply to the protected health information of a deceased individual following the death of that individual.

Response: We find the arguments raised by these commenters persuasive. We have reconsidered our position and believe these arguments for maintaining privacy on protected health information without temporal limitations outweigh any administrative burdens associated with maintaining such protections. As such, in the final rule we revise our policy to extend protections on the protected health information about a deceased individual to remain in effect for as long as the covered entity maintains the information.

For purposes of this regulation, this means that, except for uses and disclosures for research purposes (see § 164.512(i)), covered entities must under this rule protect the protected health information about a deceased individual in the same manner and to the same extent as required for the protected health information of living individuals. This policy alleviates the burden on the covered entity from having to determine whether or not the person has died and if so, how long ago, when determining whether or not the information can be released.

Comment: One commenter asked us to delete our standard for deceased individuals, asserting that the deceased have no constitutional right to privacy and state laws are sufficient to maintain protections for protected health information about deceased individuals.

Response: We understand that traditional privacy law has historically stripped privacy protection on information at the time the subject of the information dies. However, as we pointed out in the preamble to the proposed rule, the dramatic proliferation of electronic-based interchanges and maintenance of information has enabled easier and more ready access to information that once may have been de facto protected for most people because of the difficulty of its collection and aggregation. It is also our understanding that current state laws vary widely with regard to the privacy protection of a deceased individual's individually identifiable health information. Some are less protective than others and may not take into account the implications of disclosure of genetic and hereditary information on living individuals. For these reasons, a regulatory standard is needed here in order to adequately protect the privacy interests of those who are living.

Comment: Another commenter expressed concern over the administrative problems that the proposed standard would impose, particularly in the field of retrospective health research.

Response: For certain research purposes, we permit a covered entity to use and disclose the protected health information of a deceased individual without authorization by a personal representative and absent review by an IRB or privacy board. The verification standard (§ 164.514(h)) requires that covered entities obtain an oral or written representation that the protected health information sought will be used or disclosed solely for research, and § 164.512(i)(1)(iii) requires the covered entity to obtain from the researcher documentation of the death of the individual. We believe the burden on the covered entity will be small, because it can reasonably rely on the representation of purpose and documentation of death presented by the researcher.

Comment: A few commenters argued that the standard in the proposed rule would cause significant administrative burdens on their record retention and storage policies. Commenters explained that they have internal policy record-retention guidelines which do not envision the retention of records beyond a few years. Some commenters complained about the burden of having to track dates of death, as the commenters are not routinely notified when an individual has died.

Response: The final rule does not dictate any record retention requirements for the records of deceased individuals. Since we have modified the NPRM to cover protected health information about deceased individuals for as long as the covered entity maintains the information, there will be no need for the covered entity to track dates of death.

Comment: A few commenters voiced support for the approach proposed in the proposal to maintain protections for a period of two years.

Response: After consideration of public comments, we chose not to retain this approach because the two-year period would be both inadequate and arbitrary. As discussed above, we agree with commenter arguments in support of providing indefinite protection.

Comment: A few commenters expressed concern that the regulations may be interpreted as providing a right of access to a deceased's records only for a two-year period after death. They asked the Department to clarify that the right of access of an individual, including the representatives of a deceased individual, exists for the entire period the information is held by a covered entity.

Response: We agree with these comments, given the change in policy discussed above.

Comment: A few commenters suggested that privacy protections on protected health information about deceased individuals remain in effect for a specified time period longer than 2 years, arguing that two years was not long enough to protect the privacy rights of living individuals. These commenters, however, were not in agreement as to what other period of protection should be imposed, suggesting various durations from 5 to 20 years.

Response: We chose not to extend protections in this way because specifying another time period would raise many of the same concerns voiced by the commenters regarding our proposed two year period and would not reduce the administrative burden of having to track or learn dates of death. We believe that the policy in this final rule extending protections for as long as the covered entity maintains the information addresses commenter concerns regarding the need for increased protections on the protected health information about the deceased.

Comment: Some commenters asserted that information on the decedent from the death certificate is important for assessment and research purposes and requested that the Department clarify accordingly that death certificate data be allowed for use in traditional public health assessment activities.

Response: Nothing in the final rule impedes reporting of death by covered entities as required or authorized by other laws, or access to death certificate data to the extent that such data is available publicly from non-covered entities. Death certificate data maintained by a covered entity is protected health information and must only be used or disclosed by a covered entity in accordance with the requirements of this regulation. However, the final rule permits a covered entity to disclose protected health information about a deceased individual for research purposes without authorization and absent IRB or privacy board approval.

Comment: A few commenters asked that we include in the regulation a mechanism to provide for notification of date of death. These commenters questioned how a covered entity or business partner would be notified of a death and subsequently be able to determine whether the two-year period of protection had expired and if they

were permitted to use or disclose the protected health information about the deceased. One commenter further stated that absent such a mechanism, a covered entity would continue to protect the information as if the individual were still living. This commenter recommended that the burden for providing notification and confirmation of death be placed on any authorized entity requesting information from the covered entity beyond the two-year period.

Response: In general, such notification is no longer necessary as, except for uses and disclosures for research purposes, the final rule protects the protected health information about a deceased individual for as long as the covered entity holds the record. With regard to uses and disclosures for research, the researcher must provide covered entities with appropriate documentation of proof of death, the burden is not on the covered entity.

Comment: A few commenters pointed to the sensitivity of genetic and hereditary information and its potential impact on the privacy of living relatives as a reason for extending protections on the information about deceased individuals for as long as the covered entity maintains the information. However, a few commenters recommended additional protections for genetic and hereditary information. For example, one commenter suggested that researchers should be able to use sensitive information of the deceased but then be required to publish findings in de-identified form. Another commenter recommended that protected health information about a deceased individual be protected as long as it implicates health problems that could be developed by living relatives.

Response: We agree with many of the commenters regarding the sensitivity of genetic or hereditary information and, in part for this reason, extended protections on the protected health information of deceased individuals. Our reasons for retaining the exception for research are explained above.

We agree with and support the practice of publishing research findings in de-identified form. However, we cannot regulate researchers who are not otherwise covered entities in this regulation.

Comment: One commenter asked that the final rule allow for disclosure of protected health information to funeral directors as necessary for facilitating funeral and disposition arrangements. The commenter believed that our proposal could seriously disrupt a family's ability to make funeral arrangements as hospitals, hospices, and other health care providers would not be allowed to disclose the time of death and other similar information critical to funeral directors for funeral preparation. The commenter also noted that funeral directors are already precluded by state licensing regulations and ethical standards from inappropriately disclosing confidential information about the deceased.

Further, the commenter stated that funeral directors have legitimate needs for protected health information of the deceased or of an individual when death is anticipated. For example, often funeral directors are contacted when death is foreseen in order to begin the process of planning funeral arrangements and prevent unnecessary delays. In addition, the embalming of the body is affected by the medical condition of the body.

In addition, it was noted that funeral directors need to be aware of the presence of a contagious or infectious disease in order to properly advise family members of funeral and disposition options and how they may be affected by state law. For example, certain states may prohibit cremation of remains for a certain period unless the death was caused by a contagious or infectious disease, or prohibit family members from assisting in preparing the body for disposition if there is a risk of transmitting a communicable disease from the corpse.

Response: We agree that disclosures to funeral directors for the above purposes should be allowed. Accordingly, the final rule at § 164.512(g)(2) permits covered entities to disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. Such disclosures are also permitted prior to, and in reasonable anticipation of, the individual's death.

Comment: Several commenters urged that the proposed standard for deceased individuals be clarified to allow access by a family member who has demonstrated a legitimate health-related reason for seeking the information when there is no executor, administrator, or other person authorized under applicable law to exercise the right of access of the individual.

Another commenter asked that the rule differentiate between blood relatives and family members and address their different access concerns, such as with genetic information versus information about transmittable diseases. They also recommended that the regulation allow access to protected health information by blood-related relatives prior to the end of the two-year period and provide them with the authority to extend the proposed two-year period of protection if they see fit. Lastly, the commenter suggested that the regulation address the concept of when the next-of-kin may not be appropriate to control a deceased person's health information.

Response: We agree that family members may need access to the protected health information of a deceased individual, and this regulation permits such disclosure in two ways. First, a family member may qualify as a ''personal representative'' of the individual (see § 164.502(g)). Personal representatives include anyone who has authority to act on behalf of a deceased individual or such individual's estate, not just legally-appointed executors. We also allow disclosure of protected health information to health care providers for purposes of treatment, including treatment of persons other than the individual. Thus, where protected health information about a deceased person is relevant to the treatment of a family member, the family member's physician may obtain that information. Because we limit these disclosures to disclosures for treatment purposes, there is no need to distinguish between disclosure of information about communicable diseases and disclosure of genetic information.

With regard to fitness to control information, we defer to existing state and other laws that address this matter.

Section 164.502(g)—Personal Representative

Comment: It was observed that under the proposed regulation, legal representatives with ''power of attorney'' for matters unrelated to health care would have unauthorized access to confidential medical records. Commenters recommended that access to a person's protected health information be limited to those representatives with a ''power of attorney'' for health care matters only. Related comments asked that the rule limit the definition of ''power of attorney'' to include only those instruments granting specific power to deal with health care functions and health care records.

Response: We have deleted the reference to ''power of attorney.'' Under the final rule, a person is a personal representative of a living individual if, under applicable law, such person has authority to act on behalf of an individual in making decisions related to health care. ''Decisions relating to health care'' is broader than consenting to treatment on behalf of an individual;

for example, it would include decisions relating to payment for health care. We clarify that the rights and authorities of a personal representative under this rule are limited to protected health information relevant to the rights of the person to make decisions about an individual under other law. For example, if a husband has the authority only to make health care decisions about his wife in an emergency, he would have the right to access protected health information related to that emergency, but he may not have the right to access information about treatment that she had received ten years ago.

We note that the rule for deceased individuals differs from that of living individuals. A person may be a personal representative of a deceased individual if they have the authority to act on behalf of such individual or such individual's estate for any decision, not only decisions related to health care. We create a broader scope for a person who is a personal representative of a deceased individual because the deceased individual can not request that information be disclosed pursuant to an authorization, whereas a living individual can do so.

Comment: Some commenters asked that the NPRM provision allowing informal decision-makers access to the protected health information of an incapacitated individual should be maintained in the final rule.

Response: We agree with the commenters, and retain permission for covered entities to share protected health information with informal decision-makers, under conditions specified in § 164.510(b). A person need not be a personal representative for such disclosure of protected health information to be made to an informal decision-maker.

Comment: Commenters urged that individuals with mental retardation, who can provide verbal agreement or authorization, should have control over dissemination of their protected health information, in order to increase the privacy rights of such individuals.

Response: Individuals with mental retardation have control over dissemination of their protected health information under this rule to the extent that state law provides such individuals with the capacity to act on their own behalf. We note that a covered entity need not disclose information pursuant to a consent or authorization. Therefore, even if state law determines that an individual with mental retardation is not competent to act and a personal representative provides authorization for a disclosure, a covered entity may choose not to disclose such information if the individual who lacks capacity to act expresses his or her desire that such information not be disclosed.

Comment: A commenter suggested that the final rule should provide health plans with a set of criteria for formally identifying an incapacitated individual's decision-maker. Such criteria would give guidance to health plans that would help in not releasing information to the wrong person.

Response: The determination about who is a personal representative under this rule is based on state or other applicable law. We require that a covered entity verify the authority of a personal representative, in accordance with § 164.514(h) in order to disclose information to such person.

Comment: Commenters were troubled by the inclusion of minors in the definition of ''individual'' and believed that the presumption should be that parents have the right to care for their children.

Response: We agree that a parent should have access to the protected health information about their unemancipated minor children, except in limited circumstances based on state law. The approach in the final rule helps clarify this policy. The definition of ''individual'' is simplified in the final rule to ''the person who is the subject of protected health information.'' (§ 164.501). We created a new section (§ 164.502(g)) to address ''personal representatives,'' which includes parents and guardians of unemancipated minors. Generally, we provide that if under applicable law a parent has authority to act on behalf of an unemancipated minor in making decisions relating to health care about the minor, a covered entity must treat the parent as the personal representative with respect to protected health information relevant to such personal representation. The regulation provides only three limited exceptions to this rule based upon current state law and physician practice.

Comment: Many commenters agreed with our approach in the NPRM to give minors who may lawfully access health care the rights to control the protected health information related to such health care.

Several commenters disagreed with this approach and recommended that where states allow minors too much independence from parents, the rule should not defer to state law. One commenter suggested that we give an individual the right to control protected health information only when the individual reaches the age of majority.

Response: In the final rule, the parent, as the personal representative of a minor child, controls the protected health information about the minor, except that the parent does not act as a personal representative of the minor under the rule in three limited circumstances based on state consent law and physician practice. The final rule defers to consent laws of each state and does not attempt to evaluate the amount of control a state gives to a parent or minor. If a state provides an alternative means for a minor to obtain health care, other than with the consent of a parent, this rule preserves the system put in place by the state.

The first two exceptions, whereby a parent is not the personal representative for the minor and the minor can act for himself or herself under the rule, occur if the minor consents to a health care service, and no other consent to such health care service is required by law, or when the minor may lawfully obtain a health care service without the consent of a parent, and the minor, a court, or another person authorized by law consents to such service. The third exception is based on guidelines of the American Pediatric Association, current practice, and agreement by parents. If a parent assents to an agreement of confidentiality between a covered provider and a minor with respect to a health care service, the parent is not the personal representative of the minor with respect to the protected health information created or received subject to that confidentiality agreement. In such circumstances, the minor would have the authority to act as an individual, with respect to such protected health information.

Comment: Some commenters requested that we permit minors to exercise the rights of an individual when applicable law requires parental notification as opposed to parental consent.

Response: We adopt this policy in the final rule. If the minor consents to a health care service, and no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained or notification to another person has been given, only the minor may be treated as the individual with respect to the protected health information relating to such health care service. The rule does not affect state law that authorizes or requires notification to a parent of a minor's decision to obtain a health care service to the extent authorized or required by such law. In addition, state parental notification laws do not affect the rights of minors under this regulation.

Comment: Some commenters requested clarification that when a minor may obtain a health care service without parental consent and voluntarily chooses to involve a parent, the minor retains the rights, authorities and confidentiality protections established in this rule.

Response: We agree that minors should be encouraged to voluntarily involve a parent or other responsible adult in their health care decisions. The rule is not intended to require that minors choose between involving a parent and maintaining confidentiality protections. We have added language in § 164.502(g)(3)(i) to clarify that when a minor consents to a health care service and no other consent is required by law, if the minor voluntarily chooses to involve a parent or other adult, the minor nonetheless maintains the exclusive ability to exercise their rights under the rule. This is true even if a parent or other person also has consented to the health care service for which the minor lawfully consented. Under the rule, a minor may involve a parent and still preserve the confidentiality of their protected health information. In addition, a minor may choose to have a parent act as his or her personal representative even if the minor could act on his or her own behalf under the rule. If the minor requests that a covered entity treat a parent as his or her personal representative, the covered entity must treat such person as the minor's personal representative even if the minor consents to a health care service and no other consent to such health care service is required by law.

Comment: Some commenters requested that the rule provide for the preservation of patient confidences if a health care provider and a minor patient enter into an agreement of confidentiality and a parent assents to this arrangement.

Response: We have addressed this concern in the final rule by adding a provision that ensures that a minor maintains the confidentiality protections provided by the rule for information that is created or received pursuant to a confidential communication between a provider and a minor when the minor's parent assents to an agreement of confidentiality between the provider and the minor. (§ 164.502(g)(3)(ii)). The American Academy of Pediatrics Guidelines for Health Supervision III, which are meant to serve as ''a framework to help clinicians focus on important issues at developmentally appropriate time intervals,'' recommends that physicians interview children alone beginning at the age of twelve (or as early as the age of ten if it is comfortable for the child). This recommendation is based on the fact that adolescents tend to underutilize existing health care resources, in part, because of a concern for confidentiality.[7] The recommended interview technique in the Guidelines states that the provider discuss the rules of confidentiality with the adolescent and the parent and that the adolescent's confidentiality should be respected. We do not intend to interfere with these established protocols or current practices. Covered entities will need to establish procedures to separate protected health information over which the minor maintains control from protected health information with respect to which the minor's parent has rights as a personal representative of the minor.

A covered provider may disclose protected health information to a parent, regardless of a confidentiality agreement, if there is an imminent threat to the minor or another person, in accordance with § 164.512(j)(1)(i).

Comment: Several commenters suggested that we add a provision in the final rule to provide minors and parents with concurrent rights under certain circumstances, particularly when the minor reaches 16 years of age or when a parent authorizes his or her minor child to exercise these rights concurrently.

Response: We do not add such provision in the final rule. We believe that establishing concurrent rights through this rule could result in problems that effect the quality of health care if the minor and the parent were to disagree on the exercise of their rights. The rule would not prevent a parent from allowing a minor child to make decisions about his or her protected health information and acting consistently with the minor's decision. In all cases, either the parent has the right to act for the individual with respect to protected health information, or the minor has the right to act for himself or herself. The rule does not establish concurrent rights for parents and minors.

Comment: Commenters requested clarification about the rights of an adult or emancipated minor with respect to protected health information concerning health care services rendered while the person was an unemancipated minor.

Response: Once a minor becomes emancipated or attains the age of majority, as determined by applicable state law, the parent is no longer the personal representative under § 164.502(g)(3) of such individual, unless the parent has the authority to act on behalf of the individual for some reason other than their authority as a parent. An adult or emancipated minor has rights under the rule with respect to all protected health information about them, including information obtained while the individual was an unemancipated minor.

Comment: One commenter pointed out that language in the definition of individual in the NPRM that grants a minor the rights of an individual when he or she ''lawfully receives care without the consent of, or notification to, a parent * * *'' would have the effect of granting rights to an infant minor who receives emergency care when the parent is not available.

Response: This result was not our intent. We have changed the language in § 164.502(g)(3)(i) of the final rule to provide a minor the right to act as an individual when the minor can obtain care without the consent of a parent and the minor consents to such care. Because an infant treated in an emergency situation would not be able to consent to care, the infant's parent would be treated as the personal representative of the infant. Section 164.502(g)(3)(ii) provides that the parent is not the personal representative of the minor under the rule if the minor may obtain health care without the consent of a parent and the minor, a court, or another person authorized by law consents to such service. If an infant obtains emergency care without the consent of a parent, a health care provider may provide such care without consent to treatment. This situation would fall outside the second exception, and the parent would remain the personal representative of the minor.

Comment: Commenters were concerned about the interaction of this rule with FERPA with respect to parents' right to access the medical records of their children.

Response: We direct the commenters to a discussion of the interaction between our rule and FERPA in the ''Relationship to Other Federal Laws'' section of the preamble.

Section 164.502(h)—Confidential Communications

Comments on confidential communications are addressed in the preamble to § 164.522(b).

[7] Confidentiality in Adolescent Health Care, a joint policy statement of the American Academy of Pediatrics; the American Academy of Family Physicians; the American College of Obstetricians and Gynecologists; NAACOG—The Organization for Obstetric, Gynecologic, and Neonatal Nurses; and the National Medical Association.

Section 164.502(i)—Uses and Disclosures Consistent With Notice

Comments on the notice requirements are addressed in the preamble to § 164.520.

Section 164.502(j)—Uses and Disclosures by Whistleblowers and Workforce Crime Victims

Comments: Some commenters wanted to see more limitations put on the ability to whistleblow in the final rule. These commenters were concerned about how disclosed protected health information would be used during and subsequent to the whistleblowing event and felt that adding additional limitations to the ability to whistleblow would help to alleviate these concerns. Some of these commenters were concerned that there was no protection against information later being leaked to the public or re-released after the initial whistleblowing event, and that this could put covered entities in violation of the law. Many commenters wanted to see the whistleblower provision deleted entirely. According to a number of health care associations who commented on this topic, current practices already include adequate mechanisms for informing law enforcement, oversight and legal counsel of possible violations without the need for patient identifiable information; thus, the provision allowing whistleblowers to share protected health information is unnecessary. Additionally, some commenters felt that the covered entity needs to be allowed to prohibit disclosures outside of legitimate processes. Some commenters were concerned about not having any recourse if the whistleblower's suspicions were unfounded.

Response: In this rule, we do not regulate the activities of whistleblowers. Rather, we regulate the activities of covered entities, and determine when they may be held responsible under this rule for whistleblowing activities of their workforce or business associates when that whistleblowing involves the disclosure of protected health information. Similarly, we regulate when covered entities must and need not sanction their workforce who disclose protected health information in violation of the covered entity's policies and procedures, when that disclosure is for whistleblowing purposes. See § 164.530(e). This rule does not address a covered entity's recourse against a whistleblower under other applicable law.

We do not hold covered entities responsible under this rule for whistleblowing disclosures of protected health information under the circumstances described in § 164.502(j). Our purpose in including this provision is to make clear that we are not erecting a new barrier to whistleblowing, and that covered entities may not use this rule as a mechanism for sanctioning workforce members or business associates for whistleblowing activity. We do not find convincing commenters' arguments for narrowing or eliminating the scope of the whistleblowing which triggers this protection.

Congress, as well as several states, have recognized the importance of whistleblower activity to help identify fraud and mismanagement and protect the public's health and safety. Whistleblowers, by their unique insider position, have access to critical information not otherwise easily attainable by oversight and enforcement organizations.

While we recognize that in many instances, de-identified or anonymous information can be used to accomplish whistleblower objectives, there are instances, especially involving patient care and billing, where this may not be feasible. Oversight investigative agencies such as the Department of Justice rely on identifiable information in order to issue subpoenas that are enforceable. Relevant court standards require the government agency issuing the subpoena to explain why the specific records requested are relevant to the subject of the investigation, and without such an explanation the subpoena will be quashed. Issuing a subpoena for large quantities of individual records to find a few records involving fraud is cost prohibitive as well as likely being unenforceable.

We note that any subsequent inappropriate disclosure by a recipient of whistleblower information would not put the covered entity in violation of this rule, since the subsequent disclosure is not covered by this regulation.

Comments: A few commenters felt that the whistleblower should be held to a ''reasonableness standard'' rather than a ''belief'' that a violation has taken place before engaging in whistleblower activities. The commenters felt that a belief standard is too subjective. By holding the whistleblower to this higher standard, this would serve to protect protected health information from being arbitrarily released. Some commenters saw the whistleblower provision as a loophole that gives too much power to disgruntled employees to inappropriately release information in order to cause problems for the employer.

On the other hand, some commenters felt that all suspicious activities should be reported. This would ease potential whistleblowers' concerns over whether or not they had a legitimate concern by leaving this decision up to someone else. A number of commenters felt that employees should be encouraged to report violations of professional or clinical standards, or when a patient, employee, or the public would be put at risk. A small number of commenters felt that the whistleblower should raise the issue within the covered entity before going to the attorney, oversight agency, or law enforcement entity.

Response: We do not attempt to regulate the conduct of whistleblowers in this rule. We address uses and disclosures of protected health information by covered entities, and when a covered entity will violate this rule due to the actions of a workforce member or business associate. In the final rule, we provide that a covered entity is not in violation of the rule when a workforce member or business associate has a good faith belief that the conduct being reported is unlawful or otherwise violates professional or clinical standards, or potentially endangers patients, employees or the public. We concur that the NPRM language requiring only a ''belief'' was insufficient. Consequently, we have strengthened the standard to require a good faith belief that an inappropriate behavior has occurred.

Comment: A number of commenters believe that employees should be encouraged to report violations of professional or clinical standards, or report situations where patients, employees, or the public would be put at risk. Their contention is that employees, especially health care employees, may not know whether the problem they have encountered meets a legal threshold of wrongdoing, putting them at jeopardy of sanction if they are incorrect, even if the behavior did reflect violation of professional and clinical standards or put patients, employees, or the public at risk.

Response: We agree that covered entities should be protected when their employees and others engage in the conduct described by these commenters. We therefore modify the proposal to protect covered entities when the whistleblowing relates to violations of professional or clinical standards, or situations where the public may be at risk, and eliminate the reference to ''evidence.''

Comments: A significant number of those commenting on the whistleblower provision felt that this provision was contrary to the rest of the rule.

Whistleblowers could very easily release protected health information under this provision despite the fact that the rest of this rule works very hard to ensure privacy of protected health information in all other contexts. To this end, some commenters felt that whistleblowers should not be exempt from the minimum necessary requirement.

Response: As stated above, we do not regulate the conduct of whistleblowers. We discuss above the importance of whistleblowing, and our intention not to erect a new barrier to such activity. The minimum necessary standard applies to covered entities, not to whistleblowers.

Comments: Some commenters felt that disclosures of suspected violations should only be made to a law enforcement official or oversight agency. Other commenters said that whistleblowers should be able to disclose their concerns to long-term care ombudsmen or health care accreditation organizations, particularly because certain protected health information may contain evidence of abuse. Some commenters felt that whistleblowers should not be allowed to freely disclose information to attorneys. They felt that this may cause more lawsuits within the health care industry and be costly to providers. Furthermore, allowing whistleblowers to go to attorneys increases the number of people who have protected health information without any jurisdiction for the Secretary to do anything to protect this information.

Response: We agree with the commenters who suggested that we recognize other appropriate entities to which workforce members and business associates might reasonably make a whistleblowing disclosure. In the final rule we expand the provision to protect covered entities for disclosures of protected health information made to accreditation organizations by whistleblowers. We agree with the commenters that whistleblowers may see these organizations as appropriate recipients of health information, and do not believe that covered entities should be penalized for such conduct.

We also agree that covered entities should be protected when whistleblowers disclose protected health information to any health oversight agency authorized by law to investigate or oversee the conditions of the covered entity, including state Long-Term Care Ombudsmen appointed in accordance with the Older Americans Act. Among their mandated responsibilities is their duty to identify, investigate and resolve complaints that are made by, or on behalf of, residents related to their health, safety, welfare, or rights. Nursing home staff often bring complaints regarding substandard care or abuse to ombudsmen. Ombudsmen provide a potentially more attractive outlet for whistleblowers since resolution of problems may be handled short of legal action or formal investigation by an oversight agency.

We disagree with commenters that the provision permitting disclosures to attorneys is too broad. Workforce members or business associates may not understand their legal options or their legal exposure when they come into possession of information about unlawful or other inappropriate or dangerous conduct. Permitting potential whistleblowers to consult an attorney provides them with a better understanding of their legal options. We rephrase the provision to improve its clarity.

Comment: One commenter suggested that a notice of information practices that omits disclosure for voluntary reporting of fraud will chill internal whistleblowers who will be led to believe—falsely—that they would violate federal privacy law, and be lawfully subject to sanction by their employer, if they reported fraud to health oversight agencies.

Response: The notice of information practices describes a covered entity's information practices. A covered entity does not make whistleblower disclosures of protected health information, nor can it be expected to anticipate any such disclosures by its workforce.

Comment: One commenter suggested that the whistleblower provisions could allow covered entities to make illegal disclosures to police through the back door by having an employee who believes there is a violation of law do the disclosing. Any law could have been violated and the violator could be anyone (a patient, a member of the patient's family, etc.)

Response: We have eliminated whistleblower disclosures for law enforcement purposes from the list of circumstances in which the covered entity will be protected under this rule. This provision is intended to protect the covered entity when a member of its workforce or a business associate discloses protected health information to whistleblow on the covered entity (or its business associates); it is not intended for disclosures of conduct by the individual who is the subject of the information or third parties.

Section 164.504—Uses and Disclosures—Organizational Requirements—Component Entities, Affiliated Entities, Business Associates and Group Health Plans

Section 164.504(a)–(c)—Health Care Component (Component Entities) and Section 164.504(d)—Affiliated Entities

Comment: A few commenters asked that the concept of ''use'' be modified to allow uses within an integrated healthcare delivery system. Commenters argued that the rule needs to ensure that the full spectrum of treatment is protected from the need for authorizations at the points where treatment overlaps entities. It was explained that, for example, treatment for a patient often includes services provided by various entities, such as by a clinic and hospital, or that treatment may also necessitate referrals from one provider entity to another unrelated entity. Further, the commenter argued that the rule needs to ensure that the necessary payment and health care operations can be carried out across entities without authorizations.

Response: The Department understands that in today's health care industry, the organization of and relationships among health care entities are highly complex and varied. We modify the proposed rule significantly to allow affiliated entities to designate themselves as a single covered entity. A complex organization, depending on how it self-designates, may have one or several ''health care component(s)'' that are each a covered entity. Aggregation into a single covered entity will allow the entities to use a single notice of information practices and will allow providers that must obtain consent for uses and disclosures for treatment, payment, and operations to obtain a single consent.

We do not allow this type of aggregation for unrelated entities, as suggested by some commenters, because unrelated entities' information practices will be too disparate to be accurately reflected on a single consent or notice form. Our policies on when consent and authorization are required for sharing information among unrelated entities, and the rationale for these policies, is described in §§ 164.506 and 164.508 and corresponding preamble.

As discussed above, in the final rule we have added a definition of organized health care arrangement and permit covered entities participating in such arrangements to disclose protected health information to support the health care operations of the arrangement. See the preamble discussion of the definitions of organized health care

arrangement and health care operations, § 164.501.

Comment: Some commenters expressed concern that the requirement to obtain authorization for the disclosure of information to a non-health related division of the covered entity would impede covered entities' ability to engage in otherwise-permissible activities such as health care operations. Some of these commenters requested clarification that covered entities are only required to obtain authorization for disclosures to non-health related divisions if the disclosure is for marketing purposes.

Response: In the final rule, we remove the example of use and disclosure to non-health related divisions of the covered entity from the list of examples of uses and disclosures requiring authorization in § 164.508. We determined that the example could lead covered entities to the mistaken conclusion that some uses or disclosures that would otherwise be permitted under the rule without authorization would require authorization when made to a non-health related division of the covered entity. In the final rule, we clarify that disclosure to a non-health related division does not require authorization if the use or disclosure is otherwise permitted or required under the rule. For example, in § 164.501 we define health care operations to include conducting or arranging for legal and auditing services. A covered entity that is the health care component of a larger entity is permitted under the final rule to include the legal department of the larger entity as part of the health care component. The covered entity may not, however, generally permit the disclosure of protected health information from the health care component to non-health related divisions unless they support the functions of the health care component and there are policies and procedures in place to restrict the further use to the support of the health related functions.

Comment: Many commenters, especially those who employed providers, supported our position in the proposed rule to consider only the health care component of an entity to be the covered entity. They stated that this was a balanced approach that would allow them to continue conducting business. Some commenters felt that there was ambiguity in the regulation text of the proposed rule and requested that the final rule explicitly clarify that only the health care component is considered the covered entity, not the entity itself. Similarly, another commenter requested that we clarify that having a health care component alone did not make the larger entity a covered entity under the rule.

Response: We appreciate the support of the commenters on the health care component approach and we agree that there was some ambiguity in the proposed rule. The final rule creates a new § 164.504(b) for health care components. Under § 164.504(b), for a covered entity that is a single legal entity which predominantly performs functions other than the functions performed by a health plan, provider, or clearinghouse, the privacy rules apply only to the entity's health care component. A policy, plan, or program that is an ''excepted benefit'' under section 2791(c)(1) of HIPAA cannot be part of a health care component because it is expressly excluded from the definition of ''health plan'' for the reasons discussed above. The health care component is prohibited from sharing protected health information outside of the component, except as otherwise permitted or required by the regulation.

At a minimum, the health care component includes the organizational units of the covered entity that operate as or perform the functions of the health plan, health care provider, or clearinghouse and does not include any unit or function of the excepted benefits plan, policy, or program. While the covered entity remains responsible for compliance with this rule because it is responsible for the actions of its workforce, we otherwise limit the responsibility to comply to the health care component of the covered entity. The requirements of this rule apply only to the uses and disclosures of the protected health information by the component entity. See § 164.504(b).

Comment: Some commenters stated that the requirement to erect firewalls between different components would unnecessarily delay treatment, payment, and health care operations and thereby increase costs. Other commenters stressed that it is necessary to create firewalls between the health care component and the larger entity to prevent unauthorized disclosures of protected health information.

Response: We believe that the requirement to implement firewalls or safeguards is necessary to provide meaningful privacy protections, particularly because the health care component is part of a larger legal organization that performs functions other than those covered under this rule. Without the safeguard requirement we cannot ensure that the component will not share protected health information with the larger entity. While we do not specifically identify the safeguards that are required, the covered entity must implement policies and procedures to ensure that: the health care component's use and disclose of protected health information complies with the regulation; members of the health care component who perform duties for the larger entity do not use and disclose protected health information obtained through the health care component while performing non-component functions unless otherwise permitted or required by the regulation; and when a covered entity conducts multiple functions regulated under this rule, the health care component adheres to the appropriate requirements (e.g. when acting as a health plan, adheres to the health plan requirements) and uses or discloses protected health information of individuals who receive limited functions from the component only for the appropriate functions. See §§ 164.504(c)(2) and 164.504(g). For example, a covered entity that includes both a hospital and a health plan may not use protected health information obtained from an individual's hospitalization for the health plan, unless the individual is also enrolled in the health plan. We note that covered entities are permitted to make a disclosure to a health care provider for treatment of an individual without restrictions.

Comment: One commenter stated that multiple health care components of a single organization should be able to be treated as a single component entity for the purposes of this rule. Under this approach, they argued, one set of policies and procedures would govern the entire component and protected health information could be shared among components without authorization. Similarly, other commenters stated that corporate subsidiaries and affiliated entities should not be treated as separate covered entities.

Response: We agree that some efficiencies may result from designating multiple component entities as a single covered entity. In the final rule we allow legally distinct covered entities that share common ownership or control to designate themselves or their health care components as a single covered entity. See § 164.504(d). Common ownership is defined as an ownership or equity interest of five percent or more. Common control exists if an entity has the power—directly or indirectly—to significantly influence or direct the actions or policies of another entity. If the affiliated entity contains health care components, it must implement safeguards to prevent the

larger entity from using protected health information maintained by the component entity. As stated above, organizations that perform multiple functions may designate a single component entity as long as it does not include the functions of an excepted benefit plan that is not covered under the rule. In addition, it must adhere to the appropriate requirements when performing its functions (e.g. when acting as a health plan, adhere to the health plan requirements) and uses or discloses protected health information of individuals who receive limited functions from the component only for the appropriate functions. At the same time, a component that is outside of the health care component may perform activities that otherwise are not permitted by a covered entity, as long as it does not use or disclose protected health information created or received by or on behalf of the health care component in ways that violate this rule.

Comment: Some commenters asked whether or not workers' compensation carriers could be a part of the health care component as described in the proposed rule. They argued that this would allow for sharing of information between the group health plan and workers' compensation insurers.

Response: Under HIPAA, workers' compensation is an excepted benefit program and is excluded from the definition of ''health plan.'' As such, a component of a covered entity that provides such excepted benefits may not be part of a health care component that performs the functions of a health plan. If workforce members of the larger entity perform functions for both the health care component and the non-covered component, they may not use protected health information created or received by or on behalf of the health care component for the purposes of the non-covered component, unless otherwise permitted by the rule. For example, information may be shared between the components for coordination of benefits purposes.

C*omment:* Several commenters requested specific guidance on identifying the health care component entity. They argued that we underestimated the difficulty in determining the component and that many organizations have multiple functions with the same people performing duties for both the component and the larger entity.

Response: With the diversity of organizational structures, it is impossible to provide a single specific guidance for identifying health care components that will meet the needs of all organizations. Covered entities must designate their health care components consistent with the definition at § 164.504(a). We have tried to frame this definition to delineate what comes within a health care component and what falls outside the component.

Comment: A commenter representing a government agency recommended that only the component of the agency that runs the program be considered a covered entity, not the agency itself. In addition, this commenter stated that often subsets of other government agencies work in partnership with the agency that runs the program to provide certain services. For example, one state agency may provide maternity support services to the Medicaid program which is run by a separate agency. The commenter read the rule to mean that the agency providing the maternity support services would be a business associate of the Medicaid agency, but was unclear as to whether it would also constitute a health care component within its own agency.

Response: We generally agree. We expect that in most cases, government agencies that run health plans or provide health care services would typically meet the definition of a ''hybrid entity'' under § 164.504(a), so that such an agency would be required to designate the health care component or components that run the program or programs in question under § 164.504(c)(3), and the rules would not apply to the remainder of the agency's operations, under § 164.504(b). In addition, we have created an exception to the business associate contract requirement for government agencies who perform functions on behalf of other government agencies. Government agencies can enter into a memorandum of understanding with another government entity or adopt a regulation that applies to the other government entity in lieu of a business associate contract, as long as the memorandum or regulation contains certain terms. See § 164.504(e).

Comment: One commenter representing an insurance company stated that different product lines should be treated separately under the rule. For example, the commenter argued, because an insurance company offers both life insurance and health insurance, it does not mean that the insurance company itself is a covered entity, rather only the health insurance component is a covered entity. Another commenter requested clarification of the use of the term ''product line'' in the proposed rule. This commenter stated that product line should differentiate between different lines of coverage such as life vs. health insurance, not different variations of the same coverage, such as HMO vs. PPO. Finally, one commenter stated that any distinction among product lines is unworkable because insurance companies need to share information across product lines for coordinating benefits. This sharing of information, the commenter urged, should be able to take place whether or not all product lines are covered under the rule.

Response: We agree that many forms of insurance do not and should not come within the definition of ''health plan,'' and we have excepted them from the definition of this term in § 160.103 applies. This point is more fully discussed in connection with that definition. Although we do not agree that the covered entity is only the specific product line, as this comment suggests, the hybrid entity rules in § 164.504 address the substance of this concern. Under § 164.504(c)(3), an entity may create a health plan component which would include all its health insurance lines of business or separate health care components for each health plan product line. Finally, the sharing of protected health information across lines of business is allowed if it meets the permissive or required disclosures under the rule. The commenter's example of coordination of benefits would be allowed under the rule as payment.

Comment: Several commenters representing occupational health care providers supported our use of the component approach to prohibit unauthorized disclosures of protected health information. They requested that the regulation specifically authorize them to deny requests for disclosures outside of the component entity when the disclosure was not otherwise permitted or required by the regulation.

Response: We appreciate the commenters' support of the health care component approach. As members of a health care component, occupational health providers are prohibited from sharing protected health information with the larger entity (i.e., the employer), unless otherwise permitted or required by the regulation.

Comment: One commenter asked how the regulation affects employers who carry out research. The commenter questioned whether the employees carrying out the research would be component entities under the rule.

Response: If the employer is gathering its own information rather than obtaining it from an entity regulated by this rule, the information does not constitute protected health information since the employer is not a covered

entity. If the employer is obtaining protected health information from a covered entity, the disclosure by the covered entity must meet the requirements of § 164.512(i) regarding disclosures for research.

Comment: One commenter stated that the proposed rule did not clearly articulate whether employees who are health care providers are considered covered entities when they collect and use individually identifiable health information acting on behalf of an employer. Examples provided include, administering mandatory drug testing, making fitness-for-duty and return-to-work determinations, testing for exposure to environmental hazards, and making short and long term disability determinations. This commenter argued that if disclosing information gained through these activities requires authorization, many of the activities are meaningless. For example, an employee who fails a drug test is unlikely to give authorization to the provider to share the information with the employer.

Response: Health care providers are covered entities under this rule if they conduct standard transactions. A health care provider who is an employee and is administering drug testing on behalf of the employer, but does not conduct standard transactions, is not a covered entity. If the health care provider is a covered entity, then we require authorization for the provider to disclose protected health information to an employer. Nothing in this rule, however, prohibits the employer from conditioning an individual's employment on agreeing to the drug testing and requiring the individual to sign an authorization allowing his or her drug test results to be disclosed to the employer.

Comment: One commenter stated its belief that only a health center at an academic institution would be a covered entity under the component approach. This commenter believed it was less clear whether or not other components that may create protected health information ''incidentally'' through conducting research would also become covered entities.

Response: While a covered entity must designate as a health care component the functions that make it a health care provider, the covered entity remains responsible for the actions of its workforce. Components that create protected health information through research would be covered entities to the extent they performed one of the required transactions described in § 164.500; however, it is possible that the research program would not be part of the health care component, depending on whether the research program performed or supported covered functions.

Comment: Several commenters stated that employers need access to protected health information in order to provide employee assistance programs, wellness programs, and on-site medical testing to their employees.

Response: This rule does not affect disclosure of health information by employees to the employer if the information is not obtained from a covered entity. The employer's access to information from an EAP, wellness program, or on-site medical clinic will depend on whether the program or clinic is a covered entity.

Comment: One commenter stated that access to workplace medical records by the occupational medical physicians is fundamental to workplace and community health and safety. Access is necessary whether it is a single location or multiple sites of the same company, such as production facilities of a national company located throughout the country.

Response: Health information collected by the employer directly from providers who are not covered entities is outside the scope of this regulation. We note that the disclosures which this comment concerns should be covered by § 164.512(b).

Section 164.504(e)—Business Associates

Comment: Many commenters generally opposed the business partner standard and questioned the Secretary's legal authority under section 1172(a) of HIPAA to require business partner contracts. Others stated that the proposed rule imposed too great a burden on covered entities with regard to monitoring their business partners' actions. Commenters stated that they did not have the expertise to adequately supervise their business partners' activities—including billing, accounting, and legal activities—to ensure that protected health information is not inappropriately disclosed. Commenters argued that business partners are not ''under the control'' of health care providers, and that the rule would significantly increase the cost of medical care. Many commenters stated that the business partner provisions would be very time consuming and expensive to implement, noting that it is not unusual for a health plan or hospital to have hundreds of business partners, especially if independent physicians and local pharmacies are considered business partners. Many physician groups pointed out that their business partners are large providers, hospitals, national drug supplier and medical equipment companies, and asserted that it would be impossible, or very expensive, for a small physician group to attempt to monitor the activity of large national companies. Commenters stated that complex contract terms and new obligations would necessitate the investment of significant time and resources by medical and legal personnel, resulting in substantial expenses. Many commenters proposed that the duty to monitor be reduced to a duty to terminate the contractual arrangement upon discovery of a failure to comply with the privacy requirements.

In addition, many commenters argued that covered entities should have less responsibility for business partners' actions regarding the use and disclosure of protected health information. The proposed rule would have held covered entities responsible for the actions of their business partners when they ''knew or reasonably should have known'' of improper use of protected health information and failed to take reasonable steps to cure a breach of the business partner contract or terminate the contract. Many commenters urged that the term ''knew or should have known'' be clearly defined, with examples. Some commenters stated that covered entities should be liable only when they have actual knowledge of the material breach of the privacy rules by the business partner. Others recommended creation of a process by which a business partner could seek advice to determine if a particular disclosure would be appropriate. Some commenters stated that, in order to create an environment that would encourage covered entities to report misuses of protected health information, a covered entity should not be punished if it discovered an inappropriate disclosure.

Response: With regard to our authority to require business associate contracts, we clarify that Congress gave the Department explicit authority to regulate what uses and disclosures of protected health information by covered entities are ''authorized.'' If covered entities were able to circumvent the requirements of these rules by the simple expedient of contracting out the performance of various functions, these rules would afford no protection to individually identifiable health information and be rendered meaningless. It is thus reasonable to place restrictions on disclosures to business associates that are designed to ensure that the personal medical information disclosed to them continues to be protected and used and further

disclosed only for appropriate (i.e., permitted or required) purposes.

We do not agree that business associate contracts would necessarily have complex terms or result in significant time and resource burdens. The implementation specifications for business associate contracts set forth in § 164.504 are straightforward and clear. Nothing prohibits covered entities from having standard contract forms which could require little or no modification for many business associates.

In response to comments that the ''knew or should have known'' standard in the proposed rule was too vague or difficult to apply, and concerns that we were asking too much of small entities in monitoring the activities of much larger business associates, we have changed the rule. Under the final rule, we put responsibility on the covered entity to take action when it ''knew of a pattern of activity or practice of the business associate that constituted, respectively, a material breach or violation of the business associate's obligation under the contract * * *'' This will preclude confusion about what a covered entity 'should have known.' We interpret the term ''knew'' to include the situation where the covered entity has credible evidence of a violation. Covered entities cannot avoid responsibility by intentionally ignoring problems with their contractors. In addition, we have eliminated the requirement that a covered entity actively monitor and ensure protection by its business associates. However, a covered entity must investigate credible evidence of a violation by a business associate and act upon any such knowledge.

In response to the concern that the covered entity should not be punished if it discovers an inappropriate disclosure by its business associate, § 164.504(e) provides that the covered entity is not in compliance with the rule if it fails to take reasonable steps to cure the breach or end the violation, while § 164.530(f) requires the covered entity to mitigate, to the extent practicable, any resultant harm. The breach itself does not cause a violation of this rule.

Comment: Some commenters voiced support for the concept of business partners. Moreover, some commenters urged that the rule apply directly to those entities that act as business partners, by restricting disclosures of protected health information after a covered entity has disclosed it to a business partner.

Response: We are pleased that commenters supported the business associate standard and we agree that there are advantages to legislation that directly regulates most entities that use or disclose protected health information. However, we reiterate that our jurisdiction under the statute limits us to regulate only those covered entities listed in § 160.102.

Comment: Many commenters strongly opposed the provision in the proposed rule requiring business partner contracts to state that individuals whose protected health information is disclosed under the contract are intended third party beneficiaries of the contract. Many noted that HIPAA did not create a private right of action for individuals to enforce a right to privacy of medical information, and questioned the Secretary's authority to create such a right through regulation. Others questioned whether the creation of such a right was appropriate in light of the inability of Congress to reach consensus on the question, and perceived the provision as a ''back door'' attempt to create a right that Congress did not provide. Some commenters noted that third party beneficiary law varies from state to state, and that a third party beneficiary provision may be unenforceable in some states. These commenters suggested that the complexity and variation of state third party beneficiary law would increase cost and confusion with limited privacy benefits.

Commenters predicted that the provision would result in a dramatic increase in frivolous litigation, increased costs throughout the health care system, and a chilling effect on the willingness of entities to make authorized disclosures of protected information. Many commenters predicted that fear of lawsuits by individuals would impede the flow of communications necessary for the smooth operation of the health care system, ultimately affecting quality of care. For example, some predicted that the provision would inhibit providers from making authorized disclosures that would improve care and reduce medical errors. Others predicted that it would limit vendors' willingness to support information systems requirements. One large employer stated that the provision would create a substantial disincentive for employers to sponsor group health plans. Another commenter noted that the provision creates an anomaly in that individuals may have greater recourse against business partners and covered entities that contract with them than against covered entities acting alone.

However, some commenters strongly supported the concept of providing individuals with a mechanism to enforce the provisions of the rule, and considered the provision among the most important privacy protections in the proposed rule.

Response: We eliminate the requirement that business associate contracts contain a provision stating that individuals whose protected health information is disclosed under the contract are intended third-party beneficiaries of the contract.

We do not intend this change to affect existing laws regarding when individuals may be third party beneficiaries of contracts. If existing law allows individuals to claim third party beneficiary rights, or prohibits them from doing so, we do not intend to affect those rules. Rather, we intend to leave this matter to such other law.

Comment: Some commenters objected to the proposed rule's requirement that the business partner must return or destroy all protected health information received from the covered entity at the termination of the business partner contract. Commenters argued that business partners will need to maintain business records for legal and/or financial auditing purposes, which would preclude the return or destruction of the information. Moreover, they argued that computer back-up files may contain protected health information, but business partners cannot be expected to destroy entire electronic back-up files just because part of the information that they contain is from a client for whom they have completed work.

Response: We modify the proposed requirement that the business associate must return or destroy all protected health information received from the covered entity when the business associate contract is terminated. Under the final rule, a business associate must return or destroy all protected health information when the contract is terminated if feasible and lawful. The business partner contract must state that privacy protections continue after the contract ends, if there is a need for the business associate to retain any of the protected health information and for as long as the information is retained. In addition, the permissible uses of information after termination of the contract must be limited to those activities that make return or destruction of the information not feasible.

Comment: Many commenters recommended that providers and plans be excluded from the definition of ''business partner'' if they are already governed by the rule as covered entities. Providers expressed particular concern about the inclusion of physicians with hospital privileges as business partners of the hospital, as each hospital would

be required to have written contracts with and monitor the privacy practices of each physician with privileges, and each physician would be required to do the same for the hospital. Another commenter argued that consultations between covered entities for treatment or referral purposes should not be subject to the business partner contracting requirement.

Response: The final rule retains the general requirement that, subject to the exceptions below, a covered entity must enter into a business associate contract with another covered entity when one is providing services to or acting on behalf of the other. We retain this requirement because we believe that a covered entity that is a business associate should be restricted from using or disclosing the protected health information it creates or receives through its business associate function for any purposes other than those that are explicitly detailed in its contract.

However, the final rule expands the proposed exception for disclosures of protected health information by a covered health care provider to another health care provider. The final rule allows such disclosures without a business associate contract for any activities that fall under the definition of ''treatment.'' We agree with the commenter that the administrative burdens of requiring contracts in staff privileges arrangements would not be outweighed by any potential privacy enhancements from such a requirement. Although the exception for disclosure of protected health information for treatment could be sufficient to relieve physicians and hospitals of the contract requirement, we also believe that this arrangement does not meet the true meaning of ''business associate,'' because both the hospital and physician are providing services to the patient, not to each other. We therefore also add an exception to § 164.502(e)(1) that explicitly states that a contract is not required when the association involves a health care facility and another health care provider with privileges at that facility, if the purpose is providing health care to the individual. We have also added other exceptions in § 164.502(e)(1)(ii) to the requirement to obtain ''satisfactory assurances'' under § 164.502(e)(1)(i). We do not require a business associate arrangement between group health plans and their plan sponsors because other, albeit analogous, requirements apply under § 164.504(f) that are more tailored to the specifics of that legal relationship. We do not require business associate arrangements between government health plans providing public benefits and other agencies conducting certain functions for the health plan, because these arrangements are typically very constrained by other law.

Comment: Many commenters expressed concern that required contracts for federal agencies would adversely affect oversight activities, including investigations and audits. Some health plan commenters were concerned that if HMOs are business partners of an employer then the employer would have a right to all personal health information collected by the HMO. A commenter wanted to be sure that authorization would not be required for accreditation agencies to access information. A large manufacturing company wanted to make sure that business associate contracts were not required between affiliates and a parent corporation that provides administrative services for a sponsored health plan. Attorney commenters asserted that a business partner contract would undermine the attorney/client relationship, interfere with attorney/client privilege, and was not necessary to protect client confidences. A software vendor wanted to be excluded because the requirements for contracts were burdensome and government oversight intrusive. Some argued that because the primary purpose of medical device manufacturers is supplying devices, not patient care, they should be excluded.

Response: We clarify in the above discussion of the definition of ''business associate'' that a health insurance issuer or an HMO providing health insurance or health coverage to a group health plan does not become a business associate simply by providing health insurance or health coverage. The health insurance issuer or HMO may perform additional functions or activities or provide additional services, however, that would give rise to a business associate relationship. However, even when an health insurance issuer or HMO acts as a business associate of a group health plan, the group health plan has no right of access to the other protected health information maintained by the health insurance issuer or HMO. The business associate contract must constrain the uses and disclosures of protected health information obtained by the business associate through the relationship, but does not give the covered entity any right to request the business associate to disclose protected health information that it maintains outside of the business associate relationship to the group health plan. Under HIPAA, employers are not covered entities, so a health insurance issuer or HMO cannot act as a business associate of an employer. See § 164.504(f) with respect to disclosures to plan sponsors from a group health plan or health insurance issuer or HMO with respect to a group health plan.

With respect to attorneys generally, the reasons the commenters put forward to exempt attorneys from this requirement were not persuasive. The business associate requirements will not prevent attorneys from disclosing protected health information as necessary to find and prepare witness, nor from doing their work generally, because the business associate contract can allow disclosures for these purposes. We do not require business associate contracts to identify each disclosure to be made by the business associate; these disclosures can be identified by type or purpose. We believe covered entities and their attorneys can craft agreements that will allow for uses and disclosures of protected health information as necessary for these activities. The requirement for a business associate contract does not interfere with the attorney-client relationship, nor does it override professional judgement of business associates regarding the protected health information they need to discharge their responsibilities. We do not require covered entities to second guess their professional business associates' reasonable requests to use or disclose protected health information in the course of the relationship.

The attorney-client privilege covers only a small portion of information provided to attorneys and so is not a substitute for this requirement. More important, attorney-client privilege belongs to the client, in this case the covered entity, and not to the individual who is the subject of the information. The business associate requirements are intended to protect the subject of the information.

With regard to government attorneys and other government agencies, we recognize that federal and other law often does not allow standard legal contracts among governmental entities, but instead requires agreements to be made through the Economy Act or other mechanisms; these are generally reflected in a memorandum of understanding (MOU). We therefore modify the proposed requirements to allow government agencies to meet the required ''satisfactory assurance'' through such MOUs that contain the same provisions required of business associate contracts. As discussed elsewhere, we believe that direct regulation of entities receiving protected health information can be as or more effective in protecting health

information as contracts. We therefore also allow government agencies to meet the required ''satisfactory assurances'' if law or regulations impose requirements on business associates consistent with the requirements specified for business associate contracts.

We do not believe that the requirement to have a business associate contract with agencies that are performing the specified services for the covered entity or undertaking functions or activities on its behalf undermines the government functions being performed. A business associate arrangement requires the business associate to maintain the confidentiality of the protected health information and generally to use and disclose the information only for the purposes for which it was provided. This does not undermine government functions. We have exempted from the business associate requirement certain situations in which the law has created joint uses or custody over health information, such as when law requires another government agency to determine the eligibility for enrollment in a covered health plan. In such cases, information is generally shared across a number of government programs to determine eligibility, and often is jointly maintained. We also clarify that health oversight activities do not give rise to a business associate relationship, and that protected health information may be disclosed by a covered entity to a health oversight agency pursuant to § 164.512(d).

We clarify for purposes of the final rule that accreditation agencies are business associates of a covered entity and are explicitly included within the definition. During accreditation, covered entities disclose substantial amounts of protected health information to other private persons. A business associate contract basically requires the business associate to maintain the confidentiality of the protected health information that it receives and generally to use and disclose such information for the purposes for which it was provided. As with attorneys, we believe that requiring a business associate contract in this instance provides substantial additional privacy protection without interfering with the functions that are being provided by the business associate.

With regard to affiliates, § 164.504(d) permits affiliates to designate themselves as a single covered entity for purposes of this rule. (See § 164.504(d) for specific organizational requirements.) Affiliates that choose to designate themselves as a single covered entity for purposes of this rule will not need business associate contracts to share protected health information. Absent such designation, affiliates are business associates of the covered entity if they perform a function or service for the covered entity that necessitates the use or disclosure of protected health information.

Software vendors are business associates if they perform functions or activities on behalf of, or provide specified services to, a covered entity. The mere provision of software to a covered entity would not appear to give rise to a business associate relationship, although if the vendor needs access to the protected health information of the covered entity to assist with data management or to perform functions or activities on the covered entity's behalf, the vendor would be a business associate. We note that when an employee of a contractor, like a software or IT vendor, has his or her primary duty station on-site at a covered entity, the covered entity may choose to treat the employee of the vendor as a member of the covered entity's workforce, rather than as a business associate. See the preamble discussion to the definition of workforce, § 160.103.

With regard to medical device manufacturers, we clarify that a device manufacturer that provides ''health care'' consistent with the rule's definition, including being a ''supplier'' under the Medicare program, is a health care provider under the final rule. We do not require a business associate contract when protected health information is shared among health care providers for treatment purposes. However, a device manufacturer that does not provide ''health care'' must be a business associate of a covered entity if that manufacturer receives or creates protected health information in the performance of functions or activities on behalf of, or the provision of specified services to, a covered entity.

As to financial institutions, they are business associates under this rule when they conduct activities that cause them to meet the definition of business associate. See the preamble discussion of the definition of ''payment'' in § 164.501, for an explanation of activities of a financial institution that do not require it to have a business associated contract.

Disease managers may be health care providers or health plans, if they otherwise meet the respective definitions and perform disease management activities on their own behalf. However, such persons may also be business associates if they perform disease management functions or services for a covered entity.

Comment: Other commenters recommended that certain entities be included within the definition of ''business partner,'' such as transcription services; employee representatives; in vitro diagnostic manufacturers; private state and comparative health data organizations; state hospital associations; warehouses; ''whistleblowers,'' credit card companies that deal with health billing; and patients.

Response: We do not list all the types of entities that are business associates, because whether an entity is a business associate depends on what the entity does, not what the entity is. That is, this is a definition based on function; any entity performing the function described in the definition is a business associate. Using one of the commenters' examples, a state hospital association may be a business associate if it performs a service for a covered entity for which protected health information is required. It is not a business associate by virtue of the fact that it is a hospital association, but by virtue of the service it is performing.

Comment: A few commenters urged that certain entities, i.e., collection agencies and case managers, be business partners rather than covered entities for purposes of this rule.

Response: Collection agencies and case managers are business associates to the extent that they provide specified services to or perform functions or activities on behalf of a covered entity. A collection agency is not a covered entity for purposes of this rule. However, a case manager may be a covered entity because, depending on the case manager's activities, the person may meet the definition of either a health care provider or a health plan. See definitions of ''health care provider'' and ''health plan'' in § 164.501.

Comment: Several commenters complained that the proposed HIPAA security regulation and privacy regulation were inconsistent with regard to business partners.

Response: We will conform these policies in the final Security Rule.

Comment: One commenter expressed concern that the proposal appeared to give covered entities the power to limit by contract the ability of their business partners to disclose protected health information obtained from the covered entity regardless of whether the disclosure was permitted under proposed § 164.510, ''Uses and disclosures for which individual authorization is not required'' (§ 164.512 in the final rule). Therefore, the commenter argued that the covered

entity could prevent the business partner from disclosing protected health information to oversight agencies or law enforcement by omitting them from the authorized disclosures in the contract.

In addition, the commenter expressed concern that the proposal did not authorize business partners and their employees to engage in whistleblowing. The commenter concluded that this omission was unintended since the proposal's provision at proposed § 164.518(c)(4) relieved the covered entity, covered entity's employees, business partner, and the business partner's employees from liability for disclosing protected health information to law enforcement and to health oversight agencies when reporting improper activities, but failed to specifically authorize business partners and their employees to engage in whistleblowing in proposed § 164.510(f), ''Disclosures for law enforcement.''

Response: Under our statutory authority, we cannot directly regulate entities that are not covered entities; thus, we cannot regulate most business associates, or 'authorize' them to use or disclose protected health information. We agree with the result sought by the commenter, and accomplish it by ensuring that such whistle blowing disclosures by business associates and others do not constitute a violation of this rule on the part of the covered entity.

Comment: Some commenters suggested that the need to terminate contracts that had been breached would be particularly problematic when the contracts were with single-source business partners used by health care providers. For example, one commenter explained that when the Department awards single-source contracts, such as to a Medicare carrier acting as a fiscal intermediary that then becomes a business partner of a health care provider, the physician is left with no viable alternative if required to terminate the contract.

Response: In most cases, we expect that there will be other entities that could be retained by the covered entity as a business associate to carry out those functions on its behalf or provide the necessary services. We agree that under certain circumstances, however, it may not be possible for a covered entity to terminate a contract with a business associate. Accordingly, although the rule still generally requires a covered entity to terminate a contract if steps to cure such a material breach fail, it also allows an exception to this to accommodate those infrequent circumstances where there simply are no viable alternatives to continuing a contract with that particular business associate. It does not mean, however, that the covered entity can choose to continue the contract with a non-compliant business associate merely because it is more convenient or less costly than doing business with other potential business associates. We also require that if a covered entity determines that it is not feasible to terminate a non-compliant business associate, the covered entity must notify the Secretary.

Comment: Another commenter argued that having to renegotiate every existing contract within the 2-year implementation window so a covered entity can attest to ''satisfactory assurance'' that its business partner will appropriately safeguard protected health information is not practical.

Response: The 2-year implementation period is statutorily required under section 1175(b) of the Act. Further, we believe that two years provides adequate time to come into compliance with the regulation.

Comment: A commenter recommended that the business partner contract specifically address the issue of data mining because of its increasing prevalence within and outside the health care industry.

Response: We agree that protected health information should only be used by business associates for the purposes identified in the business associate contract. We address the issue of data mining by requiring that the business associate contract explicitly identify the uses or disclosures that the business associate is permitted to make with the protected health information. Aside from disclosures for data aggregation and business associate management, the business associate contract cannot authorize any uses or disclosures that the covered entity itself cannot make. Therefore, data mining by the business associate for any purpose not specified in the contract is a violation of the contract and grounds for termination of the contract by the covered entity.

Comment: One commenter stated that the rule needs to provide the ability to contract with persons and organizations to complete clinical studies, provide clinical expertise, and increase access to experts and quality of care.

Response: We agree, and do not prohibit covered entities from sharing protected health information under a business associate contract for these purposes.

Comment: A commenter requested clarification as to whether sister agencies are considered business partners when working together.

Response: It is unclear from the comment whether the ''sister agencies'' are components of a larger entity, are affiliated entities, or are otherwise linked. Requirements regarding sharing protected health information among affiliates and components are found in § 164.504.

Comment: One commenter stated that some union contracts specify that the employer and employees jointly conduct patient quality of care reviews. The commenter requested clarification as to whether this arrangement made the employee a business partner.

Response: An employee organization that agrees to perform quality assurance for a group health plan meets the definition of a business associate. We note that the employee representatives acting on behalf of the employee organization would be performing the functions of the organization, and the employee organization would be responsible under the business associate contract to ensure that the representatives abided by the restrictions and conditions of the contract. If the employee organization is a plan sponsor of the group health plan, the similar provisions of § 164.504(f) would apply instead of the business associate requirements. See § 164.502(e)(1).

Comment: Some commenters supported regulating employers as business partners of the health plan. These commenters believed that this approach provided flexibility by giving employers access to information when necessary while still holding employers accountable for improper use of the information. Many commenters, however, stressed that this approach would turn the relationship between employers, employees and other agents ''on its head'' by making the employer subordinate to its agents. In addition, several commenters objected to the business partner approach because they alleged it would place employers at risk for greater liability.

Response: We do not require a business associate contract for disclosure of protected health information from group health plans to employers. We do, however, put other conditions on the disclosure of protected health information from group health plans to employers who sponsor the plan. See further discussion in § 164.504 on disclosure of protected health information to employers.

Comment: One commenter expressed concern that the regulation would discourage organizations from participating with Planned Parenthood since pro bono and volunteer services may have no contract signed.

Response: We design the rule's requirements with respect to volunteers and pro bono services to allow flexibility to the covered entity so as not to disturb these arrangements. Specifically, when such volunteers work on the premises of the covered entity, the covered entity may choose to treat them as members of the covered entity's workforce or as business associates. See the definitions of business associate and workforce in § 160.103. If the volunteer performs its work off-site and needs protected health information, a business associate arrangement will be required. In this instance, where protected health information leaves the premises of the covered entity, privacy concerns are heightened and it is reasonable to require an agreement to protect the information. We believe that pro bono contractors will easily develop standard contracts to allow those activities to continue smoothly while protecting the health information that is shared.

Section 164.504(f)—Group Health Plans

Comment: Several commenters interpreted the preamble in the proposed rule to mean that only self-insured group health plans were covered entities. Another commenter suggested there was an error in the definition of group health plans because it only included plans with more than 50 participants *or* plans administered by an entity other than the employer (emphasis added by commenter). This commenter believed the ''or'' should be an ''and'' because almost all plans under 50 are administered by another entity and therefore this definition does not exclude most small plans.

Response: We did not intend to imply that only self-insured group health plans are covered health plans. We clarify that all group health plans, both self-insured and fully-funded, with 50 or more participants are covered entities, and that group health plans with fewer than 50 participants are covered health plans if they are administered by another entity. While we agree with the commenter that few group health plans with fewer than 50 participants are self-administered, the ''or'' is dictated by the statute. Therefore, the statute only exempts group health plans with fewer than 50 participants that are not administered by an entity other than the employer.

Comment: Several commenters stated that the proposed rule mis-characterized the relationship between the employer and the group health plan. The commenters stated that under ERISA and the Internal Revenue Code group health plans are separate legal entities from their employer sponsors. The group health plan itself, however, generally does not have any employees. Most operations of the group health plan are contracted out to other entities or are carried out by employees of the employer who sponsors the plan. The commenters stressed that while group health plans are clearly covered entities, the Department does not have the statutory authority to cover employers or other entities that sponsor group health plans. In contrast, many commenters stated that without covering employers, meaningful privacy protection is unattainable.

Response: We agree that group health plans are separate legal entities from their plan sponsors and that the group health plan itself may be operated by employees of the plan sponsor. We make significant modification to the proposed rule to better reflect this reality. We design the requirements in the final regulation to use the existing regulatory tools provided by ERISA, such as the plan documents required by that law and the constellation of plan administration functions defined by that law that established and maintain the group health plan.

We recognize plan sponsors' legitimate need for health information in certain situations while, at the same time, protecting health information from being used for employment-related functions or for other functions related to other employee benefit plans or other benefits provided by the plan sponsor. We do not attempt to directly regulate plan sponsors, but pursuant to our authority to regulate health plans, we place restrictions on the flow of information from covered entities to non-covered entities. The final rule permits group health plans to disclose protected health information to plan sponsors, and allows them to authorize health insurance issuers or HMOs to disclose protected health information to plan sponsors, if the plan sponsors agree to use and disclose the information only as permitted or required by the regulation. The information may be used only for plan administration functions performed on behalf of the group health plan and specified in the plan documents. Hereafter, any reference to employer in a response to a comment uses the term ''plan sponsor,'' since employers can only receive protected health information in their role as plan sponsors, except as otherwise permitted under this rule, such as with an authorization.

Specifically, in order for a plan sponsor to obtain without authorization protected health information from a group health plan, health insurance issuer, or HMO, the documents under which the group health plan was established and is maintained must be amended to: (1) Describe the permitted uses and disclosures of protected health information by the plan sponsor (see above for further explanation); (2) specify that disclosure is permitted only upon receipt of a written certification that the plan documents have been amended; and (3) provide adequate firewalls. The firewalls must identify the employees or classes of employees or other persons under the plan sponsor's control who will have access to protected health information; restrict access to only the employees identified and only for the administrative functions performed on behalf of the group health plan; and provide a mechanism for resolving issues of noncompliance by the employees identified. Any employee of the plan sponsor who receives protected health information in connection with the group health plan must be included in the amendment to the plan documents. As required by ERISA, the named fiduciary is responsible for ensuring the accuracy of amendments to the plan documents.

Group health plans, and health insurance issuers or HMOs with respect to the group health plan, that disclose protected health information to plan sponsors are bound by the minimum necessary standard as described in § 164.514.

Group health plans, to the extent they provide health benefits only through an insurance contract with a health insurance issuer or HMO and do not create, receive, or maintain protected health information (except for summary information or enrollment and disenrollment information), are not required to comply with the requirements of §§ 164.520 or 164.530, except for the documentation requirements of § 164.530(j). In addition, because the group health plan does not have access to protected health information, the requirements of §§ 164.524, 164.526, and 164.528 are not applicable. Individuals enrolled in a group health plan that provides benefits only through an insurance contract with a health insurance issuer or HMO would have access to all rights provided by this regulation through the health insurance issuer or HMO, because they are covered entities in their own right.

Comment: We received several comments from self-insured plans who stated that the proposed rule did not fully appreciate the dual nature of an employer as a plan sponsor and as a insurer. These commenters stated that

the regulation should have an exception for employers who are also insurers.

Response: We believe the approach we have taken in the final rule recognizes the special relationship between plan sponsors and group health plans, including group health plans that provide benefits through a self-insured arrangement. The final rule allows plan sponsors and employees of plan sponsors access to protected health information for purposes of plan administration. The group health plan is bound by the permitted uses and disclosures of the regulation, but may disclose protected health information to plan sponsors under certain circumstances. To the extent that group health plans do not provide health benefits through an insurance contract, they are required to establish a privacy officer and provide training to employees who have access to protected health information, as well as meet the other applicable requirements of the regulation.

Comment: Some commenters supported our position not to require individual consent for employers to have access to protected health information for purposes of treatment, payment, and health care operations. For employer sponsored insurance to continue to exist as it does today, the commenters stressed, this policy is essential. Other commenters encouraged the Department to amend the regulation to require authorization for disclosure of information to employers. These commenters stressed that because the employer was not a covered entity, individual consent is the only way to prohibit potential abuses of information.

Response: In the final regulation, we maintain the position in the proposed rule that a health plan, including a group health plan, need not obtain individual consent for use and disclosure of protected health information for treatment, payment and or health care operations purposes. However, we impose conditions (described above) for making such disclosures to the plan sponsor. Because employees of the plan sponsor often perform health care operations and payment (e.g. plan administration) functions, such as claims payment, quality review, and auditing, they may have legitimate need for such information. Requiring authorization from every participant in the plan could make such fundamental plan administration activities impossible. We therefore impose regulatory restrictions, rather than a consent requirement, to prevent abuses. For example, the plan sponsor must certify that any protected health information obtained by its employees through such plan administration activities will not be used for employment-related decisions.

Comment: Several commenters stressed that the regulation must require the establishment of firewalls between group health plans and employers. These commenters stated that firewalls were necessary to prevent the employer from accessing information improperly and using it in making job placements, promotions, and firing decisions. In addition, one commenter stated that employees with access to protected health information must be empowered through this regulation to deny unauthorized access to protected health information to corporate managers and executives.

Response: We agree with the commenters that firewalls are necessary to prevent unauthorized use and disclosure of protected health information. Among the conditions for group health plans to disclose information to plan sponsors, the plan sponsor must establish firewalls to prevent unauthorized uses and disclosures of information. The firewalls include: describing the employees or classes of employees with access to protected health information; restricting access to and use of the protected health information to the plan administration functions performed on behalf of the group health plan and described in plan documents; and providing an effective mechanism for resolving issues of noncompliance.

Comment: Several commenters supported our proposal to cover the health care component of an employer in its capacity as an administrator of the group health plan. These commenters felt the component approach was necessary to prevent the disclosure of protected health information to other parts of the employer where it might be used or disclosed improperly. Other commenters believed the component approach was unworkable and that distinguishing who was in the covered entity would not be as easy as assumed in the proposed rule. One commenter stated it was unreasonable for an employer to go through its workforce division by division and employee by employee designating who is included in the component and who is not. In addition, some commenters argued that we did not have the statutory authority to regulate employers at all, including their health care components.

One commenter requested more guidance with respect to identifying the health care component as proposed under the proposed rule. In particular, the commenter requested that the regulation clearly define how to identify such persons and what activities and functional areas may be included. The commenter alleged that identification of persons needing access to protected health information will be administratively burdensome. Another commenter requested clarification on distinguishing the component entity from non-component entities within an organization and how to administer such relationships. The commenter stated that individuals included in the covered entity could change on a daily basis and advocated for a simpler set of rules governing intra-organizational relationships as opposed to inter-organizational relationships.

Response: While we have not adopted the component approach for plan sponsors in the final rule, plan sponsors who want protected health information must still identify who in the organization will have access to the information. Several of the changes we make to the NPRM will make this designation easier. First, we move from ''component'' to a more familiar functional approach. We limit the employees of the plan sponsor who may receive protected health information to those employees performing plan administration functions, as that term is understood with respect to ERISA compliance, and as limited by this rule's definitions of payment and health care operation. We also allow designation of a class of employees (e.g., all employees assigned to a particular department) or individual employees.

Although some commenters have asked for guidance, we have intentionally left the process flexible to accommodate different organizational structures. Plan sponsors may identify who will have access to protected health information in whatever way best reflects their business needs as long as participants can reasonably identify who will have access. For example, persons may be identified by naming individuals, job titles (e.g. Director of Human Resources), functions (e.g. employees with oversight responsibility for the outside third party claims administrator), divisions of the company (e.g. Employee Benefits) or other entities related to the plan sponsor. We believe this flexibility will also ease any administrative burden that may result from the identification process. Identification in terms such as ''individuals who from time to time may need access to protected health information'' or in other broad or generic ways, however, would not be sufficient.

Comment: In addition to the comments on the component approach itself, several commenters pointed out

that many employees wear two hats in the organization, one for the group health plan and one for the employer. The commenters stressed that these employees should not be regulated when they are performing group health plan functions. This arrangement is necessary, particularly in small employers where the plan fiduciary may also be in charge of other human resources functions. The commenter recommended that employees be allowed access to information when necessary to perform health plan functions while prohibiting them from using the information for non-health plan functions.

Response: We agree with the commenters that many employees perform multiple functions in an organization and we design these provisions specifically to accommodate this way of conducting business. Under the approach taken in the final regulation, employees who perform multiple functions (i.e. group health plan and employment-related functions) may receive protected health information from group health plans, but among other things, the plan documents must certify that these employees will not use the information for activities not otherwise permitted by this rule including for employment-related activities.

Comment: Several commenters pointed out that the amount of access needed to protected health information varies greatly from employer to employer. Some employers may perform many plan administration functions themselves which are not possible without access to protected health information. Other employers may simply offer health insurance by paying a premium to a health insurance issuer rather than provide or administer health benefits themselves. Some commenters argued that fully insured plans should not be covered under the rule. Similarly, some commenters argued that the regulation was overly burdensome on small employers, most of whom fully insure their group health plans. Other commenters pointed out that health insurance issuers—even in fully insured arrangements—are often asked for identifiable health information, sometimes for legitimate purposes such as auditing or quality assurance, but sometimes not. One commenter, representing an insurer, gave several examples of employer requests, including claims reports for employees, individual and aggregate amounts paid for employees, identity of employees using certain drugs, and the identity, diagnosis and anticipated future costs for ''high cost'' employees. This same commenter requested guidance in what types of information can be released to employers to help them determine the organization's responsibilities and liabilities.

Response: In the final regulation we recognize the diversity in plan sponsors' need for protected health information. Many plan sponsors need access to protected health information to perform plan administration functions, including eligibility and enrollment functions, quality assurance, claims processing, auditing, monitoring, trend analysis, and management of carve-out plans (such as vision and dental plans). In the final regulation we allow group health plans to disclose protected health information to plan sponsors if the plan sponsor voluntarily agrees to use the information only in accordance with the purposes stated in the plan documents and as permitted by the regulation. We clarify, however, that plan administration does not include any employment-related decisions, including fitness for duty determinations, or duties related to other employee benefits or plans. Plan documents may only permit health insurance issuers to disclose protected health information to a plan sponsor as is otherwise permitted under this rule and consistent with the minimum necessary standard.

Some plan sponsors, including those with a fully insured group health plan, do not perform plan administration functions on behalf of group health plans, but still may require health information for other purposes, such as modifying, amending or terminating the plan or soliciting bids from prospective issuers or HMOs. In the ERISA context actions undertaken to modify, amend or terminate a group health plan may be known as ''settlor'' functions (see *Lockheed Corp.* v. *Spink,* 517 U.S. 882 (1996)). For example, a plan sponsor may require access to information to evaluate whether to adopt a three-tiered drug formulary. Additionally, a prospective health insurance issuer may need claims information from a plan sponsor in order to provide rating information. The final rule permits plan sponsors to receive summary health information with identifiers removed in order to carry out such functions. Summary health information is information that summarizes the claims history, expenses, or types of claims by individuals enrolled in the group health plan. In addition, the identifiers listed in § 164.514(b)(2)(i) must be removed prior to disclosing the information to a plan sponsor for purposes of modifying, amending, or terminating the plan. See § 164.504(a). This information does not constitute de-identified information because there may be a reasonable basis to believe the information is identifiable to the plan sponsor, especially if the number of participants in the group health plan is small. A group health plan, however, may not permit an issuer or HMO to disclose protected health information to a plan sponsor unless the requirement in § 164.520 states that this disclosure may occur.

Comment: Several commenters stated that health insurance issuers cannot be held responsible for employers' use of protected health information. They stated that the issuer is the agent of the employer and it should not be required to monitor the employer's use and disclosure of information.

Response: Under this regulation, health insurance issuers are covered entities and responsible for their own uses and disclosures of protected health information. A group health plan must require a health insurance issuer or HMO providing coverage to the group health plan to disclose information to the plan sponsor only as provided in the plan documents.

Comment: Several commenters urged us to require de-identified information to be used to the greatest extent possible when information is being shared with employers.

Response: De-identified information is not sufficient for many functions plan sponsors perform on behalf of their group health plans. We have created a process to allow plan sponsors and their employees access to protected health information when necessary to administer the plan. We note that all uses and disclosures of protected health information by the group health plan are bound by the minimum necessary standard.

Comment: One commenter representing church plans argued that the regulation should treat such plans differently from other group health plans. The commenter was concerned about the level of access to information the Secretary would have in performing compliance reviews and suggested that a higher degree of sensitivity is need for information related to church plans than information related to other group health plans. This sensitivity is needed, the commenter alleged, to reduce unnecessary intrusion into church operations. The commenter also advocated that church plans found to be out of compliance should be able to self-correct within a stated time frame (270 days) and avoid paying penalty taxes as allowed in the Internal Revenue Code.

Response: We do not believe there is sufficient reason to treat church plans differently than other covered entities.

The intent of the compliance reviews is to determine whether or not the plan is abiding by the regulation, not to gather information on the general operations of the church. As required by § 160.310(c), the covered entity must provide access only to information that is pertinent to ascertaining compliance with part 160 or subpart E of 164.

Comment: Several commenters stated that employers often advocate on behalf of their employees in benefit disputes and appeals, answer questions with regard to the health plan, and generally help them navigate their health benefits. These commenters questioned whether this type of assistance would be allowed under the regulation, whether individual consent was required, and whether this intervention would make them a covered entity.

Response: The final rule does nothing to hinder or prohibit plan sponsors from advocating on behalf of group health plan participants or providing assistance in understanding their health plan. Under the privacy rule, however, the plan sponsor could not obtain any information from the group health plan or a covered provider unless authorization was given. We do not believe obtaining authorization when advocating or providing assistance will be impractical or burdensome since the individual is requesting assistance and therefore should be willing to provide authorization. Advocating on behalf of participants or providing other assistance does not make the plan sponsor a covered entity.

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

Comment: Many commenters supported regulatory authorization for treatment, payment, and health care operations. In particular, health plans, employers, and institutional providers supported the use of regulatory authorization for treatment, payment, and health care operations.

In contrast, a large number of commenters, particularly health care professionals, patients, and patient advocates, suggested that consent for treatment, payment, and health care operations should be required. Many commenters supported the use of consent for treatment, payment, and health care operations, considering this a requirement for maintaining the integrity of the health care system. Some commenters made a distinction between requiring and permitting providers to obtain consent.

Commenters nearly uniformly agreed that covered health care providers, health plans, and clearinghouses should not be prohibited from seeking authorization for treatment, payment, and health care operations. Some commenters stated that the prohibition against obtaining an authorization goes against professional ethics, undermines the patient-provider relationship, and is contrary to current industry practice.

Some commenters specifically noted the primacy of the doctor-patient relationship regarding consent. In general, commenters recommended that individually identifiable health information not be released by doctors without patient consent. A few commenters stated that prohibiting health care providers from obtaining consent could cause the patient to become suspicious and distrustful of the health care provider. Other commenters believed that clinicians have the responsibility for making sure that patients are fully informed about the consequences of releasing information. A few commented that the process of obtaining consent provided an opportunity for the patient and provider to negotiate the use and disclosure of patient information.

Commenters discussed how, when, and by whom consent should be sought. For example, some commenters viewed a visit between a health care provider and patient as the appropriate place for consent to be discussed and obtained. While others did not necessarily dispute the appropriateness of health care providers obtaining consent for uses and disclosures of protected health information from individuals, some said that it was appropriate for health plans to be permitted to obtain consent.

Response: In the NPRM we stated our concern that the blanket consents that individuals sign today provide these individuals with neither notice nor control over how their information is to be used. While we retain those concerns, we also understand that for many who participate in the health care system, the acts of providing and obtaining consent represent important values that these parties wish to retain. Many individuals argued that providing consent enhances their control; many advocates argued that the act of consent focuses patient attention on the transaction; and many health care providers argued that obtaining consent is part of ethical behavior.

The final rule amends our proposed approach and requires most covered health care providers to obtain a consent from their patients to use or disclose protected health information for treatment, payment, and health care operations. Providers who have an indirect treatment relationship with the patient, as defined in § 164.501, cannot be expected to have an opportunity to obtain consent and may continue to rely on regulatory authorization for their uses and disclosures for these purposes.

As described in the comments, it is the relationship between the health care provider and the patient that is the basis for many decisions about uses and disclosures of protected health information. Much of the individually identifiable health information that is the subject of this rule is created when a patient interacts with a health care provider. By requiring covered providers to obtain consent for treatment, payment, and health care operations, the individual will have appropriate opportunity to consider the appropriate uses and disclosures of his or her protected health information. We also require that the consent contain a reference to the provider's notice, which contains a more detailed description of the provider's practices relating to uses and disclosures of protected health information. This combination provides the basis for an individual to have an informed conversation with his or her provider and to request restrictions.

It is our understanding that it is common practice for providers to obtain consent for this type of information-sharing today. Many providers and provider organizations stated that they are ethically obligated to obtain the patient's consent and that it is their practice to do so. A 1998 study by Merz, et al, published in the Journal of Law, Medicine and Ethics examined hospital consent forms regarding disclosure of medical information.[8] They found that 97% of all hospitals seek consent for the release of information for payment purposes; 45% seek consent for disclosure for utilization review, peer review, quality assurance, and/or prospective review; and 50% seek consent for disclosure to providers, other health care facilities, or others for continuity of care purposes. All of these activities fall within our definitions of treatment, payment, or health care operations.

In the final rule we have not required that health plans or health care clearinghouses obtain consent for their uses and disclosures of protected health information for treatment, payment, or health care operations. The rationale underlying the consent requirements for uses and disclosures by health care providers do not pertain to health plans and health care clearinghouses. First, current practice is varied, and there is little history of health plans obtaining

[8] J. Merz, P. Sankar, S.S. Yoo, ''Hospital Consent for Disclosure of Medical Records,'' Journal of Law, Medicine & Ethics, 26 (1998): 241–248.

consent relating to their own information practices unless required to do so by some other law. This is reflected in the public comments, in which most health plans supported the regulatory authorization approach proposed in the NPRM. Further, unlike many health care providers, health plans did not maintain that they were ethically obligated to seek the consent of their patients for their use and disclosure activities. Finally, it is the unique relationship between an individual and his or her health care provider that provides the foundation for a meaningful consent process. Requiring that consent process between an individual and a health plan or clearinghouse, when no such unique relationship exists, we believe is not necessary.

Unlike their relationship with health care providers, individuals in most instances do not have a direct opportunity to engage in a discussion with a health plan or clearinghouse at the time that they enter into a relationship with those entities. Most individuals choose a health plan through their employer and often sign up through their employer without any direct contact with the health plan. We concluded that providing for a signed consent in such a circumstance would add little to the proposed approach, which would have required health plans to provide a detailed notice to their enrollees. In the final rule, we also clarify that an individual can request a restriction from a health plan or health care clearinghouse. Since individuals rarely if ever have any direct contact with clearinghouses, we concluded that requiring a signed consent would have virtually no effect beyond the provision of the notice and the opportunity to request restrictions.

We agree with the comments we received objecting to the provision prohibiting covered entities from obtaining consent from individuals. As discussed above, in the final rule we require covered health care providers with direct treatment relationships to obtain consent to use or disclose protected health information for treatment, payment, and health care operations. In addition, we have eliminated the provision prohibiting other covered entities from obtaining such consents. We note that the consents that covered entities are permitted to obtain relate to their own uses and disclosures of protected health information for treatment, payment, and health care operations and not to the practices of others. If a covered entity wants to obtain the individual's permission to receive protected health information from another covered entity, it must do so using an authorization under § 164.508.

''Consent'' versus ''Authorization''

Comment: In general, commenters did not distinguish between ''consent'' and ''authorization.'' Commenters used both terms to refer to the individual's giving permission for the use and disclosure of protected health information by any entity.

Response: In the final rule we have made an important distinction between consent and authorization. Under the final rule, we refer to the process by which a covered entity seeks agreement from an individual regarding how it will use and disclose the individual's protected health information for treatment, payment, and health care operations as ''consent.'' The provisions in the final rule relating to consent are largely contained in § 164.506. The process by which a covered entity seeks agreement from an individual to use or disclose protected health information for other purposes, or to authorize another covered entity to disclose protected health information to the requesting covered entity, are termed ''authorizations'' and the provisions relating to them are found in § 164.508.

Consent Requirements

Comment: Many commenters believed that consent might be problematic in that it could allow covered entities to refuse enrollment or services if the individual does not grant the consent. Some commenters proposed that covered entities be allowed to condition treatment, payment, or health care operations on whether or not an individual granted consent. Other commenters said that consent should be voluntary and not coerced.

Response: In the final rule (§ 164.506(b)(1)), we permit covered health care providers to condition treatment on the individual's consent to the covered provider's use or disclosure of protected health information to carry out treatment, payment, and health care operations. We recognize that it would be difficult, if not impossible, for health care providers to treat their patients and run their businesses without being able to use or disclose protected health information for these purposes. For example, a health care provider could not be reimbursed by a health plan unless the provider could share protected health information about the individual with the health plan. Under the final rule, if the individual refuses to grant consent for this disclosure, the health care provider may refuse to treat the individual. We encourage health care providers to exhaust other options, such as making alternative payment arrangements with the individual, before refusing to treat the individual on these grounds.

We also permit health plans to condition enrollment in the health plan on the individual's consent for the health plan to use and disclose protected health information to carry out treatment, payment, and health care operations (see § 164.506(b)(2)). The health plan must seek the consent in conjunction with the individual's enrollment in the plan for this provision to apply. For example, a health plan's application for enrollment may include a consent for the health plan to use or disclose protected health information to carry out treatment, payment, and/or health care operations. If the individual does not sign this consent, the health plan, under § 164.502(a)(1)(iii), is prohibited from using or disclosing protected health information about the individual for the purposes stated in the consent form. Because the health plan may not be able adequately to provide services to the individual without these uses and disclosures, we permit the health plan to refuse to enroll the individual if the consent is not signed.

Comment: Some commenters were concerned that the NPRM conflicted with state law regarding when covered entities would be required to obtain consent for uses and disclosures of protected health information.

Response: We have modified the provisions in the final rule to require certain health care providers to obtain consent for uses and disclosures for treatment, payment, and health care operations and to permit other covered entities to do so. A consent under this rule may be combined with other types of written legal permission from the individual, such as state-required consents for uses and disclosures of certain types of health information (e.g., information relating to HIV/AIDS or mental health). We also permit covered entities to seek authorization from the individual for another covered entity's use or disclosure of protected health information for these purposes, including if the covered entity is required to do so by other law. Though we do not believe any states currently require such authorizations, we wanted to avoid future conflicts. These changes should resolve the concerns raised by commenters regarding conflicts with state laws that require consent, authorization, or other types of written legal permission for uses and disclosures of protected health information.

Comment: Some commenters noted that there would be circumstances when consent is impossible or impractical. A few commenters suggested that in such situations patient information be de-identified or reviewed by an objective third party to determine if consent is necessary.

Response: Covered health care providers with direct treatment relationships are required to obtain consent to use or disclose protected health information to carry out treatment, payment, and health care operations. In certain treatment situations where the provider is permitted or required to treat an individual without the individual's written consent to receive health care, the provider may use and disclose protected health information created or obtained in the course of that treatment without the individual's consent under this rule (see § 164.506(a)(3)). In these situations, the provider must attempt to obtain the individual's consent and, if the provider is unable to obtain consent, the provider must document the attempt and the reason consent could not be obtained. Together with the uses and disclosures permitted under §§ 164.510 and 164.512, the concerns raised regarding situations in which it is impossible or impractical for covered entities to obtain the individual's permission to use or disclose protected health information about the individual have been addressed.

Comment: An agency that provides care to individuals with mental retardation and developmental disabilities expressed concern that many of their consumers lack capacity to consent to the release of their records and may not have a surrogate readily available to provide consent on their behalf.

Response: Under § 164.506(a)(3), we provide exceptions to the consent requirement for certain treatment situations in which consent is difficult to obtain. In these situations, the covered provider must attempt to obtain consent and must document the reason why consent was not obtained. If these conditions are met, the provider may use and disclose the protected health information created or obtained during the treatment for treatment, payment, or health care operations purposes, without consent.

Comment: Many commenters were concerned that covered entities working together in an integrated health care system would each separately be required to obtain consent for use and disclosure of protected health information for treatment, payment, and health care operations. These commenters recommend that the rule permit covered entities that are part of the same integrated health care system to obtain a single consent allowing each of the covered entities to use and disclose protected health information in accordance with that consent form. Some commenters said that it would be confusing to patients and administratively burdensome to require separate consents for health care systems that include multiple covered entities.

Response: We agree with commenters' concerns. In § 164.506(f) of the final rule we permit covered entities that participate in an organized health care arrangement to obtain a single consent on behalf of the arrangement. See § 164.501 and the corresponding preamble discussion regarding organized health care arrangements. To obtain a joint consent, the covered entities must have a joint notice and must refer to the joint notice in the joint consent. See § 164.520(d) and the corresponding preamble discussion regarding joint notice. The joint consent must also identify the covered entities to which it applies so that individuals will know who is permitted to use and disclose information about them.

Comment: Many commenters stated that individuals own their medical records and, therefore, should have absolute control over them, including knowing by whom and for what purpose protected health information is used, disclosed, and maintained. Some commenters asserted that, according to existing law, a patient owns the medical records of which he is the subject.

Response: We disagree. In order to assert an ownership interest in a medical record, a patient must demonstrate some legitimate claim of entitlement to it under a state law that establishes property rights or under state contract law. Historically, medical records have been the property of the health care provider or medical facility that created them, and some state statutes directly provide that medical records are the property of a health care provider or a health care facility. The final rule is consistent with current state law that provides patients access to protected health information but not ownership of medical records. Furthermore, state laws that are more stringent than the rule, that is, state laws that provide a patient with greater access to protected health information, remain in effect. See discussion of ''Preemption'' above.

Electronically Stored Data

Comment: Some commenters stated that privacy concerns would be significantly reduced if patient information is not stored electronically. One commenter suggested that consent should be given for patient information to be stored electronically. One commenter believed that information stored in data systems should not be individually identifiable.

Response: We agree that storing and transmitting health information electronically creates concerns about the privacy of health information. We do not agree, however, that covered entities should be expected to maintain health information outside of an electronic system, particularly as health care providers and health plans extend their reliance on electronic transactions. We do not believe that it would be feasible to permit individuals to opt out of electronic transactions by withholding their consent. We note that individuals can ask providers and health plans whether or not they store information electronically, and can choose only providers who do not do so or who agree not to do so. We also do not believe that it is practical or efficient to require that electronic data bases contain only de-identified information. Electronic transactions have achieved tremendous savings in the health care system and electronic records have enabled significant improvements in the quality and coordination of health care. These improvements would not be possible with de-identified information.

Section 164.508—Uses and Disclosures for Which Authorization Is Required

Uses and Disclosures Requiring Authorization

Comment: We received many comments in general support of requiring authorization for the use or disclosure of protected health information. Some comments suggested, however, that we should define those uses and disclosures for which authorization is required and permit covered entities to make all other uses and disclosures without authorization.

Response: We retain the requirement for covered entities to obtain authorization for all uses and disclosures of protected health information that are not otherwise permitted or required under the rule without authorization. We define exceptions to the general rule requiring authorization for the use or disclosure of protected health information, rather than defining narrow circumstances in which authorization is required.

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 ''each medical-care provider be considered to owe a duty of confidentiality to any individual who is the subject of a medical record it maintains, and that, therefore, no medical care provider should disclose, or be required to disclose, in individually identifiable form, any information about any such individual without the individual's explicit authorization, unless the disclosures would be'' for specifically enumerated purposes such as treatment, audit or evaluation, research, public health, and law enforcement.[9] The Commission made similar recommendations with respect to insurance institutions.[10] The Privacy Act (5 U.S.C. 552a) prohibits government agencies from disclosing records except pursuant to the written request of or pursuant to a written consent of the individual to whom the record pertains, unless the disclosure is for certain specified purposes. The National Association of Insurance Commissioners' Health Information Privacy Model Act states, ''A carrier shall not collect, use or disclose protected health information without a valid authorization from the subject of the protected health information, except as permitted by * * * this Act or as permitted or required by law or court order. Authorization for the disclosure of protected health information may be obtained for any purpose, provided that the authorization meets the requirements of this section.'' In its report ''Best Principles for Health Privacy,'' the Health Privacy Working Group stated, ''Personally identifiable health information should not be disclosed without patient authorization, except in limited circumstances' such as when required by law, for oversight, and for research.[11] The American Medical Association's Council on Ethical and Judicial Affairs has issued an opinion stating, ''The physician should not reveal confidential communications or information without the express consent of the patient, unless required to do so by law [and] subject to certain exceptions which are ethically and legally justified because of overriding social considerations.'' [12] We build on these standards in this final rule.

Comment: Some comments suggested that, under the proposed rule, a covered entity could not use protected health information to solicit authorizations from individuals. For example, a covered entity could not use protected health information to generate a mailing list for sending an authorization for marketing purposes.

Response: We agree with this concern and clarify that covered entities are permitted to use protected health information in this manner without authorization as part of the management activities relating to implementation of and compliance with the requirements of this rule. See § 164.501 and the corresponding preamble regarding the definition of health care operations.

Comment: We received several comments suggesting that we not require written authorizations for disclosures to the individual or for disclosures initiated by the individual or the individual's legal representative.

Response: We agree with this concern and in the final rule we clarify that disclosures of protected health information to the individual who is the subject of the information do not require the individual's authorization. See § 164.502(a)(1). We do not intend to impose barriers between individuals and disclosures of protected health information to them.

When an individual requests that the covered entity disclose protected health information to a third party, however, the covered entity must obtain the individual's authorization, unless the third party is a personal representative of the individual with respect to such protected health information. See § 164.502(g). If under applicable law a person has authority to act on behalf of an individual in making decisions related to health care, except under limited circumstances, that person must be treated as the personal representative under this rule with respect to protected health information related to such representation. A legal representative is a personal representative under this rule if, under applicable law, such person is able to act on behalf of an individual in making decisions related to health care, with respect to the protected health information related to such decisions. For example, an attorney of an individual may or may not be a personal representative under the rule depending on the attorney's authority to act on behalf of the individual in decisions related to health care. If the attorney is the personal representative under the rule, he may obtain a copy of the protected health information relevant to such personal representation under the individual's right to access. If the attorney is not the personal representative under the rule, or if the attorney wants a copy of more protected health information than that which is relevant to his personal representation, the individual would have to authorize such disclosure.

Comment: Commenters expressed concern about whether a covered entity can rely on authorizations made by parents on behalf of their minor children once the child has reached the age of majority and recommended that covered entities be able to rely on the most recent, valid authorization, whether it was authorized by the parent or the minor.

Response: We agree. If an authorization is signed by a parent, who is the personal representative of the minor child at the time the authorization is signed, the covered entity may rely on the authorization for as long as it is a valid authorization, in accordance with § 164.508(b). A valid authorization remains valid until it expires or is revoked. This protects a covered entity's reasonable reliance on such authorization. The expiration date of the authorization may be the date the minor will reach the age of majority. In that case, the covered entity would be required to have the individual sign a new authorization form in order to use or disclose information covered in the expired authorization form.

Comment: Some commenters were concerned that covered entities working together in an integrated system would each be required to obtain authorization separately. These commenters suggested the rule should allow covered entities that are part of the same system to obtain a single authorization allowing each of the covered entities to use and disclose protected health information in accordance with that authorization.

Response: If the rule does not permit or require a covered entity to use or disclose protected health information without the individual's authorization, the covered entity must obtain the individual's authorization to make the use or disclosure. Multiple covered entities working together as an integrated delivery system or otherwise may satisfy this requirement in at least three ways. First, each covered entity may separately obtain an authorization directly from the individual who is the subject of the protected health information to be used or disclosed. Second, one covered entity may obtain

[9] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 306.

[10] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, pp. 215–217.

[11] 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.

[12] AMA Council on Ethical and Judicial Affairs, ''Opinion E–5.05: Confidentiality,'' Issued December 1983, Updated June 1994.

a compound authorization in accordance with § 164.508(b)(3) that authorizes multiple covered entities to use and disclose protected health information. In accordance with § 164.508(c)(1)(ii), each covered entity, or class of covered entities, that is authorized to make the use or disclosure must be clearly identified. Third, if the requirements in § 164.504(d) are met, the integrated delivery system may elect to designate itself as a single affiliated covered entity. A valid authorization obtained by that single affiliated covered entity would satisfy the authorization requirements for each covered entity within the affiliated covered entity. Whichever option is used, because these authorizations are being requested by a covered entity for its own use or disclosure, the authorization must contain both the core elements in § 164.508(c) and the additional elements in § 164.508(d).

Sale, Rental, or Barter

Comment: Proposed § 164.508 listed examples of activities that would have required authorization, which included disclosure by sale, rental, or barter. Some commenters requested clarification that this provision is not intended to affect mergers, sale, or similar transactions dealing with entire companies or their individual divisions. A few commenters stated that covered entities should be allowed to sell protected health information, including claims data, as an asset of the covered entity.

Response: We clarify in the definition of health care operations that a covered entity may sell or transfer its assets, including protected health information, to a successor in interest that is or will become a covered entity. See § 164.501 and the corresponding preamble discussion regarding this change. We believe this change meets commenters' business needs without compromising individuals' privacy interests.

Comment: Some commenters supported the requirement for covered entities to obtain authorization for the sale, rental, or barter of protected health information. Some commenters argued that protected health information should never be bought or sold by anyone, even with the individual's authorization.

Response: We removed the reference to sale, rental, or barter in the final rule because we determined that the term was overly broad. For example, if a researcher reimbursed a provider for the cost of configuring health data to be disclosed under the research provisions at § 164.512(i), there may have been ambiguity that this was a sale and, therefore, required authorizations from the individuals who were the subjects of the information. We clarify in the final rule that if the use or disclosure is otherwise permitted or required under the rule without authorization, such authorization is not required simply because the disclosure is made by sale, rental, or barter.

Comment: Many commenters expressed concerns that their health information will be sold to pharmaceutical companies.

Response: Although we have removed the reference to sale, rental or barter, the final rule generally would not permit the sale of protected health information to a pharmaceutical company without the authorization of individuals who are the subjects of the information. In some cases, a covered entity could disclose protected health information to a pharmaceutical company for research purposes if the disclosure met the requirements of § 164.512(i).

Psychotherapy Notes

Comment: Public response to the concept of providing additional protections for psychotherapy notes was divided. Many individuals and most providers, particularly mental health practitioners, advocated requiring consent for use or disclosure of all or most protected health information, but particularly sensitive information such as mental health information, not necessarily limited to psychotherapy notes. Others thought there should be special protections for psychotherapy information based on the federal psychotherapist-patient privilege created by the U.S. Supreme Court in *Jaffee* v. *Redmond* and the need for an atmosphere of trust between therapist and patient that is required for effective psychotherapy. Several consumer groups recommended prohibiting disclosure of psychotherapy notes for payment purposes.

Some commenters, however, saw no need for special protections for psychotherapy communications and thought that the rules should apply the same protections for all individually identifiable information. Other commenters who advocated for no special protections based their opposition on the difficulty in drawing a distinction between physical and mental health and that special protections should be left to the states. Many health plans and employers did not support additional protections for psychotherapy notes because they stated they need access to this information to assess the adequacy of treatment, the severity of a patient's condition, the extent of a disability, or the ability to monitor the effectiveness of an individual's mental health care and eligibility for benefits. Other commenters, many from insurance companies, cited the need to have psychotherapy notes to detect fraud.

A few commenters said that it was not necessary to provide additional protections to psychotherapy notes because the ''minimum necessary'' provisions of the NPRM provide sufficient protections.

Response: In the final rule, a covered entity generally must obtain an authorization for disclosure of psychotherapy notes, or for use by a person other than the person who created the psychotherapy notes. This authorization is specific to psychotherapy notes and is in addition to the consent an individual may have given for the use or disclosure of other protected health information to carry out treatment, payment, and health care operations. This additional level of individual control provides greater protection than a general application of the ''minimum necessary'' rule. Nothing in this regulation weakens existing rules applicable to mental health information that provide more stringent protections. We do not intend to alter the holding in *Jaffee* v. *Redmond.*

Generally, we have not treated sensitive information differently from other protected health information; however, we have provided additional protections for psychotherapy notes because of *Jaffee* v. *Redmond* and the unique role of this type of information. There are few reasons why other health care entities should need access to psychotherapy notes, and in those cases, the individual is in the best position to determine if the notes should be disclosed. As we have defined them, psychotherapy notes are primarily of use to the mental health professional who wrote them, maintained separately from the medical record, and not involved in the documentation necessary to carry out treatment, payment, or health care operations. Since psychotherapy notes have been defined to exclude information that health plans would typically need to process a claim for benefits, special authorization for payment purposes should be rare. Unlike information shared with other health care providers for the purposes of treatment, psychotherapy notes are more detailed and subjective and are today subject to unique privacy and record retention practices. In fact, it is this separate existence and isolated use that allows us to grant the extra protection without causing an undue burden on the health care system.

Comment: Many commenters suggested we prohibit disclosure of psychotherapy notes without authorization for uses and disclosures under proposed § 164.510 of the NPRM, or that protections should be extended to particular uses and disclosures, such as disclosures for public health, law enforcement, health oversight, and judicial and administrative proceedings. One of these commenters stated that the only purpose for which psychotherapy notes should be disclosed without authorization is for preventing or lessening a serious or imminent threat to health or safety (proposed § 154.510(k)). Another commenter stated that the rule should allow disclosure of psychotherapy notes without authorization for this purpose, or as required by law in cases of abuse or neglect.

Other commenters did not want these protections to be extended to certain national priority activities. They claimed that information relative to psychotherapy is essential to states' activities to protect the public from dangerous mentally ill offenders and abusers, to deliver services to individuals who are unable to authorize release of health care information, and for public health assessments. One commenter requested clarification of when psychotherapy notes could be released in emergency circumstances. Several commenters stated that psychotherapy notes should not be disclosed for public health purposes.

Response: We agree with the commenters who suggested extending protections of psychotherapy notes and have limited the purposes for which psychotherapy notes may be disclosed without authorization for purposes other than treatment, payment, or health care operations. The final rule requires covered entities to obtain authorization to use or disclose psychotherapy notes for purposes listed in § 164.512, with the following exceptions: An authorization is not required for use or disclosure of psychotherapy notes when the use or disclosure is required for enforcement of this rule, in accordance with § 164.502(a)(2)(ii); when required by law, in accordance with § 164.512(a); when needed for oversight of the covered health care provider who created the psychotherapy notes, in accordance with § 164.512(d); when needed by a coroner or medical examiner, in accordance with § 164.512(g)(1); or when needed to avert a serious and imminent threat to health or safety, in accordance with § 164.512(j)(1)(i).

Comment: A commenter suggested that we follow the federal regulations governing confidentiality of alcohol and substance abuse records as a model for limited disclosure of psychotherapy notes for audits or evaluations. Under these regulations, a third party payor or a party providing financial assistance may access confidential records for auditing purposes if the party agrees in writing to keep the records secure and destroy any identifying information upon completion of the audit. (42 CFR part 2)

Response: We agree that the federal regulations concerning alcohol and drug abuse provide a good model for protection of information. However, according to our fact-finding discussions, audit or evaluation should not require access to psychotherapy notes. Protected health information kept in the medical record about an individual should be sufficient for these purposes. The final rule does not require authorization for use or disclosure of psychotherapy notes when needed for oversight of the covered health care provider who created the psychotherapy notes.

Comment: A provider organization urged that the disclosure of psychotherapy notes be strictly prohibited except to the extent needed in litigation brought by the client against the mental health professional on the grounds of professional malpractice or disclosure in violation of this section.

Response: We agree that psychotherapy notes should be available for the defense of the provider who created the notes when the individual who is the subject of the notes puts the contents of the notes at issue in a legal case. In the final rule, we allow the provider to disclose the notes to his or her lawyer for the purpose of preparing a defense. Any other disclosure related to judicial and administrative proceedings is governed by § 164.512(e).

Comment: One commenter requested that we prohibit mental health information that has been disclosed from being re-disclosed without patient authorization.

Response: Psychotherapy notes may only be disclosed pursuant to an authorization, except under limited circumstances. Covered entities must adhere to the terms of authorization and not disclose psychotherapy notes to persons other than those identified as intended recipients or for other purposes. A covered entity that receives psychotherapy notes must adhere to the terms of this rule—including obtaining an authorization for any further use or disclosure. We do not have the authority, however, to prohibit non-covered entities from re-disclosing psychotherapy notes or any other protected health information.

Comment: A provider organization argued for inclusion of language in the final rule that specifies that real or perceived ''ownership'' of the mental health record does not negate the requirement that patients must specifically authorize the disclosure of their psychotherapy notes. They cited a July 1999 National Mental Health Association survey, which found that for purposes of utilization review, every managed care plan policy reviewed ''maintains the right to access the full medical record (including detailed psychotherapy notes) of any consumer covered under its benefit plan at its whim.'' At least one of the major managed health plans surveyed considered the patient record to be the property of the health plan and governed by the health plan's policies.

Response: Although a covered entity may own a mental health record, the ability to use or disclose an individual's information is limited by state law and this rule. Under this rule, a mental health plan would not have access to psychotherapy notes created by a covered provider unless the individual who is the subject of the notes authorized disclosure to the health plan.

Comment: Some commenters expressed concern regarding the burden created by having to obtain multiple authorizations and requested clarification as to whether separate authorization for use and disclosure of psychotherapy notes is required.

Response: For the reasons explained above, we retain in the final rule a requirement that a separate authorization must be obtained for most uses or disclosures of psychotherapy notes, including those for treatment, payment, and health care operations. The burden of such a requirement is extremely low, however, because under our definition of psychotherapy notes, the need for such authorization will be very rare.

Comment: One commenter stated that Medicare should not be able to require the disclosure of psychotherapy notes because it would destroy a practitioner's ability to treat patients effectively.

Response: We agree. As in the proposed rule, covered entities may not disclose psychotherapy notes for payment purposes without an authorization. If a specific provision of law requires the disclosure of these notes, a covered entity may make the disclosure under § 164.512(a). The final rule, however, does not require the disclosure of these notes to Medicare.

Comment: One commenter expressed concern that by filing a complaint an

individual would be required to reveal sensitive information to the public. Another commenter suggested that complaints regarding noncompliance in regard to psychotherapy notes should be made to a panel of mental health professionals designated by the Secretary. This commenter also proposed that all patient information would be maintained as privileged, would not be revealed to the public, and would be kept under seal after the case is reviewed and closed.

Response: We appreciate this concern and the Secretary will ensure that individually identifiable health information and other personal information contained in complaints will not be available to the public. This Department seeks to protect the privacy of individuals to the fullest extent possible, while permitting the exchange of records required to fulfill its administrative and program responsibilities. The Freedom of Information Act, 5 U.S.C. 552, and the HHS implementing regulation, 45 CFR part 5, protect records about individuals if the disclosure would constitute an unwarranted invasion of their personal privacy, as does the Privacy Act, 5 U.S.C. 552a. See the discussion of FOIA and the Privacy Act in the ''Relationship to Other Federal Laws'' section of the preamble. Information that the Secretary routinely withholds from the public in its current enforcement activities includes individual names, addresses, and medical information. Additionally, the Secretary attempts to guard against the release of information that might involve a violation of personal privacy by someone being able to ''read between the lines'' and piece together items that would constitute information that normally would be protected from release to the public. In implementing the privacy rule, the Secretary will continue this practice of protecting personal information.

It is not clear whether the commenter with regard to the use of mental health professionals believes that such professionals should be involved because they would be best able to keep psychotherapy notes confidential or because such professionals can best understand the meaning or relevance of such notes. We anticipate that we would not have to obtain a copy or review psychotherapy notes in investigating most complaints regarding noncompliance in regard to such notes. There may be some cases in which a quick review of the notes may be needed, such as when we need to identify that the information a covered entity disclosed was in fact psychotherapy notes. If we need to obtain a copy of psychotherapy notes, we will keep these notes confidential and secure. Investigative staff will be trained in privacy to ensure that they fully respect the confidentiality of personal information. In addition, while the content of these notes is generally not relevant to violations under this rule, we will secure the expertise of mental health professionals if needed in reviewing psychotherapy notes.

Comment: A mental health organization recommended prohibiting health plans and covered health care providers from disclosing psychotherapy notes to coroners or medical examiners.

Response: In general, we have severely limited disclosures of psychotherapy notes without the individual's authorization. One case where the information may prove invaluable, but authorization by the individual is impossible and authorization by a surrogate is potentially contraindicated, is in the investigation of the death of the individual. The final rule allows for disclosures to coroners or medical examiners in this limited case.

Comment: One commenter recommended prohibiting disclosure without authorization of psychotherapy notes to government health data systems.

Response: The decision to eliminate the general provision permitting disclosures to government health data systems addresses this comment.

Comment: Several commenters were concerned that in practice, a treatment team in a mental health facility shares information about a patient in order to care for the patient and that the provision requiring authorization for use and disclosure of psychotherapy notes would expose almost all privileged information to disclosure. They requested that we add a provision that any authorization or disclosure under that statute shall not constitute a waiver of the psychotherapist-patient privilege.

Response: Because of the restricted definition we have adopted for psychotherapy notes, we do not expect that members of a team will share such information. Information shared in order to care for the patient is, by definition, not protected as psychotherapy notes. With respect to waiving privilege, however, we believe that the consents and authorizations described in §§ 164.506 and 164.508 should not be construed as waivers of a patient's evidentiary privilege. See the discussions under § 164.506 and ''Relationship to Other Laws,'' above.

Research Information Unrelated to Treatment

Definition of Research Information Unrelated to Treatment

Comment: The majority of commenters, including many researchers and health care providers, objected to the proposed definition of research information unrelated to treatment, asserting that the privacy rule should not distinguish research information unrelated to treatment from other forms of protected health information. Even those who supported the proposed distinction between research information related and unrelated to treatment suggested alternative definitions for research information unrelated to treatment.

A large number of commenters were concerned that the definition of research information unrelated to treatment was vague and unclear and, therefore, would be difficult or impossible to apply. These commenters asserted that in many instances it would not be feasible to ascertain whether research information bore some relation to treatment. In addition, several commenters asserted that the need for distinguishing research information unrelated to treatment from other forms of protected health information was not necessary because the proposed rule's general restrictions for the use and disclosure of protected health information and the existing protections for research information were sufficiently strong.

Of the commenters who supported the proposed distinction between research information related and unrelated to treatment, very few supported the proposed definition of research unrelated to treatment. A few commenters recommended that the definition incorporate a good faith provision and apply only to health care providers, because they thought it was unlikely that a health plan or health care clearinghouse would be conducting research. One commenter recommended defining research information unrelated to treatment as information which does not directly affect the treatment of the individual patient. As a means of clarifying and standardizing the application of this definition, one commenter also asserted that the definition should be based on whether the research information was for publication. In addition, one commenter specifically objected to the provision of the proposed definition that would have required that research information unrelated to treatment be information ''with respect to which the covered entity has not requested payment from

a third party payor.'' This commenter asserted that patient protection should not be dependent on whether a health plan will pay for certain care.

Response: We agree with the commenters who found the proposed definition of research information unrelated to treatment to be impractical and infeasible to apply and have eliminated this definition and its related provisions in the final rule. Although we share concerns raised by some commenters that research information generated from research studies that involve the delivery of treatment to individual subjects may need additional privacy protection, we agree with the commenters who asserted that there is not always a clear distinction between research information that is related to treatment and research information that is not. We found that the alternative definitions proposed by commenters did not alleviate the serious concerns raised by the majority of comments received on this definition.

Instead, in the final rule, we require covered entities that create protected health information for the purpose, in whole or in part, of research that includes treatment of individuals to include additional elements in authorizations they request for the use or disclosure of that protected health information. As discussed in § 164.508(f), these research-related authorizations must include a description of the extent to which some or all of the protected health information created for the research will also be used or disclosed for purposes of treatment, payment, and health care operations. For example, if the covered entity intends to seek reimbursement from the individual's health plan for the routine costs of care associated with the research protocol, it must explain in the authorization the types of information that it will provide to the health plan for this purpose. This information, and the circumstances under which disclosures will be made for treatment, payment, and health care operations, may be more limited than the information and circumstances described in the covered entity's general notice of information practices and are binding on the covered entity.

Under this approach, the covered entity that creates protected health information for research has discretion to determine whether there is a subset of research information that will have fewer allowable disclosures without authorization, and prospective research subjects will be informed about how research information about them would be used and disclosed should they agree to participate in the research study. We believe this provision in the final rule provides covered entities that participate in research necessary flexibility to enhance privacy protections for research information and provides prospective research subjects with needed information to determine whether their privacy interests would be adequately protected before agreeing to participate in a research study that involves the delivery of health care.

The intent of this provision is to permit covered entities that participate in research to bind themselves to a more limited scope of uses and disclosures for all or identified subsets of research information generated from research that involves the delivery of treatment than it may apply to other protected health information. In designing their authorizations, we expect covered entities to be mindful of the often highly sensitive nature of research information and the impact of individuals' privacy concerns on their willingness to participate in research. For example, a covered entity conducting a study which involves the evaluation of a new drug, as well as an assessment of a new un-validated genetic marker of a particular disease, could choose to stipulate in the research authorization that the genetic information generated from this study will not be disclosed without authorization for some of the public policy purposes that would otherwise be permitted by the rule under §§ 164.510 and 164.512 and by the covered entity's notice. A covered entity may not, however, include a limitation affecting its right to make a use or disclosure that is either required by law or is necessary to avert a serious and imminent threat to health or safety.

The final rule also permits the covered entity to combine the research authorization under § 164.508(f) with the consent to participate in research, such as the informed consent document as stipulated under the Common Rule or the Food and Drug Administration's human subjects regulations.

Enhance Privacy Protections for Research Information

Comment: A number of commenters argued that research information unrelated to treatment should have fewer allowable disclosures without authorization than those that would have been permitted by the proposed rule. The commenters who made this argument included those commenters who recommended that the privacy rule not cover the information we proposed to constitute research information unrelated to treatment, as well as those who asserted that the rule should cover such information. These commenters agreed with the concern expressed in the proposed rule that patients would be reluctant to participate in research if they feared that research information could be disclosed without their permission or used against them. They argued that fewer allowable disclosures should be permitted for research information because the clinical utility of the research information is most often unknown, and thus, it is unsuitable for use in clinical decision making. Others also argued that it is critical to the conduct of clinical research that researchers be able to provide individual research subjects, and the public at large, the greatest possible assurance that their privacy and the confidentiality of any individually identifiable research information will be protected from disclosure.

Several commenters further recommended that only the following uses and disclosures be permitted for research information unrelated to treatment without authorization: (1) For the oversight of the researcher or the research study; (2) for safety and efficacy reporting required by FDA; (3) for public health; (4) for emergency circumstances; or (5) for another research study. Other commenters recommended that the final rule explicitly prohibit law enforcement officials from gaining access to research records.

In addition, several commenters asserted that the rule should be revised to ensure that once protected health information was classified as research information unrelated to treatment, it could not be re-classified as something else at a later date. These commenters believed that if this additional protection were not added, this information would be vulnerable to disclosure in the future, if the information were later to gain scientific validity. They argued that individuals may rely on this higher degree of confidentiality when consenting to the collection of the information in the first instance, and that confidentiality should not be betrayed in the future just because the utility of the information has changed.

Response: We agree with commenters who argued that special protections may be appropriate for research information in order to provide research subjects with assurances that their decision to participate in research will not result in harm stemming from the misuse of the research information. We are aware that some researchers currently retain separate research records and medical records as a means of providing more stringent privacy protections for the research record. The final rule permits

covered entities that participate in research to continue to provide more stringent privacy protections for the research record, and the Secretary strongly encourages this practice to protect research participants from being harmed by the misuse of their research information.

As discussed above, in the final rule, we eliminate the special rules for this proposed definition of research information unrelated to treatment and its related provisions, so the comments regarding its application are moot.

Comment: Some commenters recommended that the final rule prohibit a covered entity from conditioning treatment, enrollment in a health plan, or payment on a requirement that the individual authorize the use or disclosure of information we proposed to constitute research information unrelated to treatment.

Response: Our decision to eliminate the definition of research information unrelated to treatment and its related provisions in the final rule renders this comment moot.

Comment: A few commenters opposed distinguishing between research information related to treatment and research information unrelated to treatment, arguing that such a distinction could actually weaken the protection afforded to clinically-related health information that is collected in clinical trials. These commenters asserted that Certificates of Confidentiality shield researchers from being compelled to disclose individually identifiable health information relating to biomedical or behavioral research information that an investigator considers sensitive.

Response: Our decision to eliminate the definition of research information unrelated to treatment and its related provisions in the final rule renders this comment moot. We would note that nothing in the final rule overrides Certificates of Confidentiality, which protect against the compelled disclosure of identifying information about subjects of biomedical, behavioral, clinical, and other research as provided by the Public Health Service Act section 301(d), 42 U.S.C. 241(d).

Privacy Protections for Research Information Too Stringent

Comment: Many of the commenters who opposed the proposed definition of research information unrelated to treatment and its related provisions believed that the proposed rule would have required authorization before research information unrelated to treatment could have been used or disclosed for any of the public policy purposes outlined in proposed § 164.510, and that this restriction would have significantly hindered many important activities. Many of these commenters specifically opposed this provision, arguing that the distinction would undermine and impede research by requiring patient authorization before research information unrelated to treatment could be used or disclosed for research.

Furthermore, some commenters recommended that the disclosure of research information should be governed by an informed consent agreement already in place as part of a clinical protocol, or its disclosure should be considered by an institutional review board or privacy board.

Response: Our decision to eliminate the definition of research information unrelated to treatment and its related provisions in the final rule renders the first two comments moot.

We disagree with the comment that suggests that existing provisions under the Common Rule are sufficient to protect the privacy interests of individuals who are subjects in research that involves the delivery of treatment. As discussed in the NPRM, not all research is subject to the Common Rule. In addition, we are not convinced that existing procedures adequately inform individuals about how their information will be used as part of the informed consent process. In the final rule, we provide for additional disclosure to subjects of research that involves the delivery of treatment as part of the research authorization under § 164.508(f). We also clarify that the research authorization could be combined with the consent to participate in research, such as the informed consent document as stipulated under the Common Rule or the Food and Drug Administration's human subjects regulations. The Common Rule (§_.116(a)(5)) requires that ''informed consent'' include ''a statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained.'' We believe that the research authorization requirements of § 164.508(f) complement the Common Rule's requirement for informed consent.

The Secretary's Authority

Comment: Several commenters, many from the research community, asserted that the coverage of ''research information unrelated to treatment'' was beyond the Department's legal authority since HIPAA did not give the Secretary authority to regulate researchers. These commenters argued that the research records held by researchers who are performing clinical trials and who keep separate research records should not be subject to the final rule. These commenters strongly disagreed that a health provider-researcher cannot carry out two distinct functions while performing research and providing clinical care to research subjects and, thus, asserted that research information unrelated to treatment that is kept separate from the medical record, would not be covered by the privacy rule.

Response: We do not agree the Secretary lacks the authority to adopt standards relating to research information, including research information unrelated to treatment. HIPAA provides authority for the Secretary to set standards for the use and disclosure of individually identifiable health information created or received by covered entities. For the reasons commenters identified for why it was not practical or feasible to divide research information into two categories—research information related to treatment and research information unrelated to treatment—we also determined that for a single research study that includes the treatment of research subjects, it is not practical or feasible to divide a researcher into two categories—a researcher who provides treatment and a researcher who does not provide treatment to research subjects. When a researcher is interacting with research subjects for a research study that involves the delivery of health care to subjects, it is not always clear to either the researcher or the research subject whether a particular research activity will generate research information that will be pertinent to the health care of the research subject. Therefore, we clarify that a researcher may also be a health care provider if that researcher provides health care, *e.g.,* provides treatment to subjects in a research study, and otherwise meets the definition of a health care provider, regardless of whether there is a component of the research study that is unrelated to the health care of the research subjects. This researcher/health care provider is then a covered entity with regard to her provider activities if she conducts standard transactions.

Valid Authorizations

Comment: In proposed § 164.508(b)(1), we specified that an authorization containing the applicable required elements ''must be accepted by the covered entity.'' A few comments requested clarification of this requirement.

Response: We agree with the commenters that the proposed provision was ambiguous and we remove it from the final rule. We note that nothing in the rule requires covered entities to act on authorizations that they receive, even if those authorizations are valid. A covered entity presented with an authorization is permitted to make the disclosure authorized, but is not required to do so.

We want to be clear, however, that covered entities will be in compliance with this rule if they use or disclose protected health information pursuant to an authorization that meets the requirements of § 164.508. We have made changes in § 164.508(b)(1) to clarify this point. First, we specify that an authorization containing the applicable required elements is a valid authorization. A covered entity may not reject as invalid an authorization containing such elements. Second, we clarify that a valid authorization may contain elements or information in addition to the required elements, as long as the additional elements are not inconsistent with the required elements.

Comment: A few comments requested that we provide a model authorization or examples of wording meeting the ''plain language'' requirement. One commenter requested changes to the language in the model authorization to avoid confusion when used in conjunction with an insurer's authorization form for application for life or disability income insurance. Many other comments, however, found fault with the proposed model authorization form.

Response: Because of the myriad of types of forms that could meet these requirements and the desire to encourage covered entities to develop forms that meet their specific needs, we do not include a model authorization form in the final rule. We intend to issue additional guidance about authorization forms prior to the compliance date. We also encourage standard-setting organizations to develop model forms meeting the requirements of this rule.

Defective Authorizations

Comment: Some commenters suggested we insert a ''good-faith reliance'' or ''substantial compliance'' standard into the authorization requirements. Commenters suggested that covered entities should be permitted to rely on an authorization as long as the individual has signed and dated the document. They stated that individuals may not fill out portions of a form that they feel are irrelevant or for which they do not have an answer. They argued that requiring covered entities to follow up with each individual to complete the form will cause unwarranted delays. In addition, commenters were concerned that large covered entities might act in good faith on a completed authorization, only to find out that a component of the entity ''knew'' some of the information on the form to be false or that the authorization had been revoked. These commenters did not feel that covered entities should be held in violation of the rule in such situations.

Response: We retain the provision as proposed and include one additional element: the authorization is invalid if it is combined with other documents in violation of the standards for compound authorizations. We also clarify that an authorization is invalid if material information on the form is known to be false. The elements we require to be included in the authorization are intended to ensure that individuals knowingly and willingly authorize the use or disclosure of protected health information about them. If these elements are missing or incomplete, the covered entity cannot know which protected health information to use or disclose to whom and cannot be confident that the individual intends for the use or disclosure to occur.

We have attempted to make the standards for defective authorizations as unambiguous as possible. In most cases, the covered entity will know whether the authorization is defective by looking at the form itself. Otherwise, the covered entity must know that the authorization has been revoked, that material information on the form is false, or that the expiration date or event has occurred. If the covered entity does not know these things and the authorization is otherwise satisfactory on its face, the covered entity is permitted to make the use or disclosure in compliance with this rule.

We have added two provisions to make it easier for covered entities to ''know'' when an authorization has been revoked. First, under § 164.508(b)(5), the revocation must be made in writing. Second, under § 164.508(c)(1)(v), authorizations must include instructions for how the individual may revoke the authorization. Written revocations submitted in the manner appropriate for the covered entity should ease covered entities' compliance burden.

Compound Authorizations

Comment: Many commenters raised concerns about the specificity of the authorization requirement. Some comments recommended that we permit covered entities to include multiple uses and disclosures in a single authorization and allow individuals to authorize or not authorize specific uses and disclosures in the authorization. Other commenters asked whether a single authorization is sufficient for multiple uses or disclosures for the same purpose, for multiple uses and disclosures for related purposes, and for uses and disclosures of different types of information for the same purpose. Some comments from health care providers noted that specific authorizations would aid their compliance with requests.

Response: As a general rule, we prohibit covered entities from combining an authorization for the use or disclosure of protected health information with any other document. For example, an authorization may not be combined with a consent to receive treatment or a consent to assign payment of benefits to a provider. We intend the authorizations required under this rule to be voluntary for individuals, and, therefore, they need to be separate from other forms of consent that may be a condition of treatment or payment or that may otherwise be coerced.

We do, however, permit covered entities to combine authorizations for uses and disclosures for multiple purposes into a single authorization. The only limitations are that an authorization for the use or disclosure of psychotherapy notes may not be combined with an authorization for the use or disclosure of other types of protected health information and that an authorization that is a condition of treatment, payment, enrollment, or eligibility may not be combined with any other authorization.

In § 164.508(b)(3), we also permit covered entities to combine an authorization for the use or disclosure of protected health information created for purposes of research including treatment of individuals with certain other documents.

We note that covered entities may only make uses or disclosures pursuant to an authorization that are consistent with the terms of the authorization. Therefore, if an individual agrees to one of the disclosures described in the compound authorization but not another, the covered entity must comply with the individual's decision. For example, if a covered entity asks an individual to sign an authorization to disclose protected health information for both marketing and fundraising purposes, but the individual only agrees to the fundraising disclosure, the

covered entity is not permitted to make the marketing disclosure.

Prohibition on Conditioning Treatment, Payment, Eligibility, or Enrollment

Comment: Many commenters supported the NPRM's prohibition of covered entities from conditioning treatment or payment on the individual's authorization of uses and disclosures. Some commenters requested clarification that employment can be conditioned on an authorization. Some commenters recommended that we eliminate the requirement for covered entities to state on the authorization form that the authorization is not a condition of treatment or payment. Some commenters suggested that we prohibit the provision of anything of value, including employment, from being conditioned on receipt of an authorization.

In addition, many commenters argued that patients should not be coerced into signing authorizations for a wide variety of purposes as a condition of obtaining insurance coverage. Some health plans, however, requested clarification that health plan enrollment and eligibility can be conditioned on an authorization.

Response: We proposed to prohibit covered entities from conditioning treatment, payment, or enrollment in a health plan on an authorization for the use or disclosure of psychotherapy notes (see proposed § 164.508(a)(3)(iii)). We proposed to prohibit covered entities from conditioning treatment or payment on authorization for the use or disclosure of any other protected health information (see proposed § 164.508(a)(2)(iii)).

We resolve this inconsistency by clarifying in § 164.508(b)(4) that, with certain exceptions, a covered entity may not condition the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on an authorization for the use or disclosure of any protected health information, including psychotherapy notes. We intend to minimize the potential for covered entities to coerce individuals into signing authorizations for the use or disclosure of protected health information when such information is not essential to carrying out the relationship between the individual and the covered entity.

Pursuant to that goal, we have created limited exceptions to the prohibition. First, a covered health care provider may condition research-related treatment of an individual on obtaining the individual's authorization to use or disclose protected health information created for the research. Second, except with respect to psychotherapy notes, a health plan may condition the individual's enrollment or eligibility in the health plan on obtaining an authorization for the use or disclosure of protected health information for making enrollment or eligibility determinations relating to the individual or for its underwriting or risk rating determinations. Third, a health plan may condition payment of a claim for specified benefits on obtaining an authorization under § 164.508(e) for disclosure to the plan of protected health information necessary to determine payment of the claim. Fourth, a covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party (such as fitness-for-duty exams and physicals necessary to obtain life insurance coverage) on obtaining an authorization for the disclosure of the protected health information. We recognize that covered entities need protected health information in order to carry out these functions and provide services to the individual; therefore, we allow authorization for the disclosure of the protected health information to be a condition of obtaining the services.

We believe that we have prohibited covered entities from conditioning the services they provide to individuals on obtaining an authorization for uses and disclosures that are not essential to those services. Due to our limited authority, however, we cannot entirely prevent individuals from being coerced into signing these forms. We do not, for example, have the authority to prohibit an employer from requiring its employees to sign an authorization as a condition of employment. Similarly, a program such as the Job Corps may make such an authorization a condition of enrollment in the Job Corps program. While the Job Corps may include a health care component, the non-covered component of the Job Corps may require as a condition of enrollment that the individual authorize the health care component to disclose protected health information to the non-covered component. See § 164.504(b). However, we note that other nondiscrimination laws may limit the ability to condition these authorizations as well.

Comment: A Medicaid fraud control association stated that many states require or permit state Medicaid agencies to obtain an authorization for the use and disclosure of protected health information for payment purposes as a condition of enrolling an individual as a Medicaid recipient. The commenter, therefore, urged an exception to the prohibition on conditioning enrollment on obtaining an authorization.

Response: As explained above, under § 164.506(a)(4), health plans and other covered entities may seek the individual's consent for the covered entity's use and disclosure of protected health information to carry out treatment, payment, or health care operations. If the consent is sought in conjunction with enrollment, the health plan may condition enrollment in the plan on obtaining the individual's consent.

Under § 164.506(a)(5), we specify that a consent obtained by one covered entity is not effective to permit another covered entity to use or disclose protected health information for payment purposes. If state law requires a Medicaid agency to obtain the individual's authorization for providers to disclose protected health information to the Medicaid agency for payment purposes, the agency may do so under § 164.508(e). This authorization must not be a condition of enrollment or eligibility, but may be a condition of payment of a claim for specified benefits if the disclosure is necessary to determine payment of the claim.

Revocation of Authorizations

Comment: Many commenters supported the right to revoke an authorization. Some comments, however, suggested that we require authorizations to remain valid for a minimum period of time, such as one year or the duration of the individual's enrollment in a health plan.

Response: We retain the right for individuals to revoke an authorization at any time, with certain exceptions. We believe this right is essential to ensuring that the authorization is voluntary. If an individual determines that an authorized use or disclosure is no longer in her best interest, she should be able to withdraw the authorization and prevent any further uses or disclosures.

Comment: Several commenters suggested that we not permit individuals to revoke an authorization if the revocation would prevent an investigation of material misrepresentation or fraud. Other commenters similarly suggested that we not permit individuals to revoke an authorization prior to a claim for benefits if the insurance was issued in reliance on the authorization.

Response: To address this concern, we include an additional exception to the right to revoke an authorization. Individuals do not have the right to revoke an authorization that was obtained as a condition of insurance coverage during any contestability

period under other law. For example, if a life insurer obtains the individual's authorization for the use or disclosure of protected health information to determine eligibility or premiums under the policy, the individual does not have the right to revoke the authorization during any period of time in which the life insurer can contest a claim for benefits under the policy in accordance with state law. If an individual were able to revoke the authorization after enrollment but prior to making a claim, the insurer would be forced to pay claims without having the necessary information to determine whether the benefit is due. We believe the existing exception for covered entities that have acted in reliance on the authorization is insufficient to address this concern because it is another person, not the covered entity, that has acted in reliance on the authorization. In the life insurance example, it is the life insurer that has taken action (i.e., issued the policy) in reliance on the authorization. The life insurer is not a covered entity, therefore the covered entity exception is inapplicable.

Comment: Some comments suggested that a covered entity that had compiled, but not yet disclosed, protected health information would have already taken action in reliance on the authorization and could therefore disclose the information even if the individual revoked the authorization.

Response: We intend for covered entities to refrain from further using or disclosing protected health information to the maximum extent possible once an authorization is revoked. The exception exists only to the extent the covered entity has taken action in reliance on the authorization. If the covered entity has not yet used or disclosed the protected health information, it must refrain from doing so, pursuant to the revocation. If, however, the covered entity has already disclosed the information, it is not required to retrieve the information.

Comment: One comment suggested that the rule allow protected health information to be only rented, not sold, because there can be no right to revoke authorization for disclosure of protected health information that has been sold.

Response: We believe this limitation would be an unwarranted abrogation of covered entities' business practices and outside the scope of our authority. We believe individuals should have the right to authorize any uses or disclosures they feel are appropriate. We have attempted to create authorization requirements that make the individual's decisions as clear and voluntary as possible.

Comment: One commenter expressed concern as to whether the proposed rule's standard to protect the protected health information about a deceased individual for two years would interfere with the payment of death benefit claims. The commenter asked that the regulation permit the beneficiary or payee under a life insurance policy to authorize disclosure of protected health information pertaining to the cause of death of a decedent or policyholder. Specifically, the commenter explained that when substantiating a claim a beneficiary, such as a fiancee or friend, may be unable to obtain the authorization required to release information to the insurer, particularly if, for example, the decedent's estate does not require probate or if the beneficiary is not on good terms with the decedent's next of kin. Further, the commenter stated that particularly in cases where the policyholder dies within two years of the policy's issuance (within the policy's contestable period) and the cause of death is uncertain, the insurer's inability to access relevant protected health information would significantly interfere with claim payments and increase administrative costs.

Response: We do not believe this will be a problem under the final regulation, because we create an exception to the right to revoke an authorization if the authorization was obtained as a condition of obtaining insurance coverage and other applicable law provides the insurer that obtained the authorization with the right to contest a claim under the policy. Thus, if a policyholder dies within the two year contestability period, the authorization the insurer obtained from the policyholder prior to death could not be revoked during the contestability period.

Core Elements and Requirements

Comment: Many commenters raised concerns about the required elements for a valid authorization. They argued that the requirements were overly burdensome and that covered entities should have greater flexibility to craft authorizations that meet their business needs. Other commenters supported the required elements as proposed because the elements help to ensure that individuals make meaningful, informed choices about the use and disclosure of protected health information about them.

Response: As in the proposed rule, we define specific elements that must be included in any authorization. We draw on established laws and guidelines for these requirements. For example, the July 1977 Report of the Privacy Protection Study Commission recommended that authorizations obtained by insurance institutions include plain language, the date of authorization, and identification of the entities authorized to disclose information, the nature of the information to be disclosed, the entities authorized to receive information, the purpose(s) for which the information may be used by the recipients, and an expiration date.[13] The Commission made similar recommendations concerning the content of authorizations obtained by health care providers.[14] The National Association of Insurance Commissioners' Health Information Privacy Model Act requires authorizations to be in writing and include a description of the types of protected health information to be used or disclosed, the name and address of the person to whom the information is to be disclosed, the purpose of the authorization, the signature of the individual or the individual's representative, and a statement that the individual may revoke the authorization at any time, subject to the rights of any person that acted in reliance on the authorization prior to revocation and provided the revocation is in writing, dated, and signed. Standards of the American Society for Testing and Materials recommend that authorizations identify the subject of the protected health information to be disclosed; the name of the person or institution that is to release the information; the name of each individual or institution that is to receive the information; the purpose or need for the information; the information to be disclosed; the specific date, event, or condition upon which the authorization will expire, unless revoked earlier; and the signature and date signed. They also recommend the authorization include a statement that the authorization can be revoked or amended, but not retroactive to a release made in reliance on the authorization.[15]

Comment: Some commenters requested clarification that authorizations ''initiated by the individual'' include authorizations initiated by the individual's representative.

---

[13] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 196–197.

[14] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 315.

[15] ASTM, ''Standard Guide for Confidentiality, Privacy, Access and Data Security, Principles for Health Information Including Computer-Based Patient Records,'' E 1869–97, § 12.1.4.

Response: In the final rule, we do not classify authorizations as those initiated by the individual versus those initiated by a covered entity. Instead, we establish a core set of elements and requirements that apply to all authorizations and require certain additional elements for particular types of authorizations initiated by covered entities.

Comment: Some commenters urged us to permit authorizations that designate a class of entities, rather than specifically named entities, that are authorized to use or disclose protected health information. Commenters made similar recommendations with respect to the authorized recipients. Commenters suggested these changes to prevent covered entities from having to seek, and individuals from having to sign, multiple authorizations for the same purpose.

Response: We agree. Under § 164.508(c)(1), we require authorizations to identify both the person(s) authorized to use or disclose the protected health information and the person(s) authorized to receive protected health information. In both cases, we permit the authorization to identify either a specific person or a class of persons.

Comment: Many commenters requested clarification that covered entities may rely on electronic authorizations, including electronic signatures.

Response: All authorizations must be in writing and signed. We intend e-mail and electronic documents to qualify as written documents. 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.

Comment: Some commenters requested that we permit covered entities to use and disclose protected health information pursuant to verbal authorizations.

Response: To ensure compliance and mutual understanding between covered entities and individuals, we require all authorizations to be in writing.

Comment: Some commenters asked whether covered entities can rely on copies of authorizations rather than the original. Other comments asked whether covered entities can rely on the assurances of a third party, such as a government entity, that a valid authorization has been obtained to use or disclose protected health information. These commenters suggested that such procedures would promote the timely provision of benefits for programs that require the collection of protected health information from multiple sources, such as determinations of eligibility for disability benefits.

Response: Covered entities must obtain the individual's authorization to use or disclose protected health information for any purpose not otherwise permitted or required under this rule. They may obtain this authorization directly from the individual or from a third party, such as a government agency, on the individual's behalf. In accordance with the requirements of § 164.530(j), the covered entity must retain a written record of authorization forms signed by the individual. Covered entities must, therefore, obtain the authorization in writing. They may not rely on assurances from others that a proper authorization exists. They may, however, rely on copies of authorizations if doing so is consistent with other law.

Comment: We requested comments on reasonable steps that a covered entity could take to be assured that the individual who requests the disclosure is whom she or he purports to be. Some commenters stated that it would be extremely difficult to verify the identity of the person signing the authorization, particularly when the authorization is not obtained in person. Other comments recommended requiring authorizations to be notarized.

Response: To reduce burden on covered entities, we are not requiring verification of the identities of individuals signing authorization forms or notarization of the forms.

Comment: A few commenters asked for clarification regarding the circumstances in which a covered entity may consider a non-response as an authorization.

Response: Non-responses to requests for authorizations cannot be considered authorizations. Authorizations must be signed and have the other elements of a valid authorization described above.

Comment: Most commenters generally supported the requirement for an expiration date on the authorization. Commenters recommended expiration dates from 6 months to 3 years and/or proposed that the expiration be tied to an event such as duration of enrollment or when an individual changes health plans. Others requested no expiration requirement for some or all authorizations.

Response: We have clarified that an authorization may include an expiration date in the form of a specific date, a specific time period, or an event directly related to the individual or the purpose of the authorization. For example, a valid authorization could expire upon the individual's disenrollment from a health plan or upon termination of a research project. We prohibit an authorization from having an indeterminate expiration date.

These changes were intended to address situations in which a specific date for the termination of the purpose for the authorization is difficult to determine. An example may be a research study where it may be difficult to predetermine the length of the project.

Comment: A few commenters requested that the named insured be permitted to sign an authorization on behalf of dependents.

Response: We disagree with the commenter that a named insured should always be able to authorize uses and disclosures for other individuals in the family. Many dependents under group health plans have their own rights under this rule, and we do not assume that one member of a family has the authority to authorize uses or disclosures of the protected health information of other family members.

A named insured may sign a valid authorization for an individual if the named insured is a personal representative for the individual in accordance with § 164.502(g). The determination of whether an individual is a personal representative under this rule is based on other applicable law that determines when a person can act on behalf of an individual in making decisions related to health care. This rule limits a person's rights and authorities as a personal representative to only the protected health information relevant to the matter for which he or she is a personal representative under other law. For example, a parent may be a personal representative of a child for most health care treatment and payment decisions under state law. In that case, a parent, who is a named insured for her minor child, would be able to provide authorization with respect to most protected health information about her dependent child. However, a wife who is the named insured for her husband who is a dependent under a health insurance policy may not be a personal representative for her husband under other law or may be a personal representative only for limited purposes, such as for making decisions regarding payment of disputed claims. In this case, she may have limited authority to access protected health information related to the payment of disputed claims, but would not have the authority to authorize that her husband's information be used for