DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160, 162, and 164

[CMS-0049-F]

RIN 0938-AI57

Health Insurance Reform: Security Standards

AGENCY: Centers for Medicare & Medicaid Services (CMS), HHS.

ACTION: Final rule.

SUMMARY: This final rule adopts standards for the security of electronic protected health information to be implemented by health plans, health care clearinghouses, and certain health care providers. The use of the security standards will improve the Medicare and Medicaid programs, and other Federal health programs and private health programs, and the effectiveness and efficiency of the health care industry in general by establishing a level of protection for certain electronic health information. This final rule implements some of the requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

DATES: Effective Date: These regulations are effective on **[OFR: insert date 60 days after the date of publication in the Federal Register].**

Compliance Date: Covered entities, with the exception of small health plans, must comply with the requirements of this final rule **[OFR: insert 24 months after the effective date of this regulation].** Small health plans must comply with the requirements of this final rule by **[OFR: insert 36 months after the effective date of this regulation].**

FOR FURTHER INFORMATION CONTACT:

William Schooler, (410) 786-0089.

SUPPLEMENTARY INFORMATION:

Availability of Copies and Electronic Access:

To order copies of the **Federal Register** containing this document, send your request to: New Orders, Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954. Specify the date of the issue requested and enclose a check or money order payable to the Superintendent of Documents, or enclose your Visa or Master Card number and expiration date. Credit card orders can also be placed by calling the order desk at (202) 512-1800 or by faxing to (202) 512-2250. The cost for each copy is $10. As an alternative, you can view and photocopy

the **Federal Register** document at most libraries designated as Federal Depository Libraries and at many other public and academic libraries throughout the country that receive the **Federal Register**.

This **Federal Register** document is also available from the **Federal Register** online database through GPO access, a service of the U.S. Government Printing Office. The website address is http://www.access.gpo.gov/nara/index.html.

I. Background

The Department of Health and Human Services (HHS) Medicare Program, other Federal agencies operating health plans or providing health care, State Medicaid agencies, private health plans, health care providers, and health care clearinghouses must assure their customers (for example, patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected. The confidentiality of health information is threatened not only by the risk of improper access to stored information, but also by the risk of interception during electronic transmission of the information. The purpose of this final

rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. Currently, no standard measures exist in the health care industry that address all aspects of the security of electronic health information while it is being stored or during the exchange of that information between entities.

This final rule adopts standards as required under title II subtitle F, sections 261 through 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191. These standards require measures to be taken to secure this information while in the custody of entities covered by HIPPA (covered entities) as well as in transit between covered entities and from covered entities to others.

The Congress included provisions to address the need for safeguarding electronic health information and other administrative simplification issues in HIPAA. In subtitle F of title II of that law, the Congress added to title XI of the Social Security Act a new part C, entitled "Administrative Simplification." (hereafter, we refer to the Social Security Act as "the Act"; we refer to the other laws cited in this document by their names). The purpose

of subtitle F is to improve the Medicare program under title XVIII of the Act, the Medicaid program under title XIX of the Act, and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements to enable the electronic exchange of certain health information.

Part C of title XI consists of sections 1171 through 1179 of the Act. These sections define various terms and impose requirements on HHS, health plans, health care clearinghouses, and certain health care providers. These statutory sections are discussed in the Transactions Rule, at 65 FR 50312, on pages 50312 through 50313, and in the final rules adopting Standards for Privacy of Individually Identifiable Health Information, published on December 28, 2000 at 65 FR 82462 (Privacy Rules), on pages 82470 through 82471, and on August 14, 2002 at 67 FR 53182. The reader is referred to those discussions.

Section 1173(d) of the Act requires the Secretary of HHS to adopt security standards that take into account the technical capabilities of record systems used to maintain health information, the costs of security measures, the need to train persons who have access to health

information, the value of audit trails in computerized record systems, and the needs and capabilities of small health care providers and rural health care providers. Section 1173(d) of the Act also requires that the standards ensure that a health care clearinghouse, if part of a larger organization, has policies and security procedures that isolate the activities of the clearinghouse with respect to processing information so as to prevent unauthorized access to health information by the larger organization. Section 1173(d) of the Act provides that covered entities that maintain or transmit health information are required to maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity and confidentiality of the information and to protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized use or disclosure of the information. These safeguards must also otherwise ensure compliance with the statute by the officers and employees of the covered entities.

II. General Overview of the Provisions of the Proposed Rule

On August 12, 1998, we published a proposed rule

(63 FR 43242) to establish a minimum standard for security of electronic health information. We proposed that the standard would require the safeguarding of all electronic health information by covered entities. The proposed rule also proposed a standard for electronic signatures. This final rule adopts only security standards. All comments concerning the proposed electronic signature standard, responses to these comments, and a final rule for electronic signatures will be published at a later date. A detailed discussion of the provisions of the August 12, 1998 proposed rule can be found at 63 FR 43245 through 43259.

We originally proposed to add part 142, entitled "Administrative requirements," to title 45 of the Code of Federal Regulations (CFR). It has now been determined that this material will reside in subchapter C of title 45, consisting of parts 160, 162, and 164. Subpart A of part 160 contains the general provisions applicable to all the Administrative Simplification rules; other subparts of part 160 will contain other requirements applicable to all standards. Part 162 contains the standards for transactions and code sets and will contain the identifier standards. Part 164 contains the standards relating to

privacy and security. Subpart A of part 164 contains general provisions applicable to part 164; subpart E contains the privacy standards. Subpart C of part 164, which is adopted in this final rule, adopts standards for the security of electronic protected health information.

III. Analysis of, and Responses to, Public Comments on the Proposed Rule

We received approximately 2,350 timely public comments on the August 12, 1998 proposed rule. The comments came from professional associations and societies, health care workers, law firms, health insurers, hospitals, and private individuals. We reviewed each commenter's letter and grouped related comments. Some comments were identical. After associating like comments, we placed them in categories based on subject matter or based on the section(s) of the regulations affected and then reviewed the comments.

In this section of the preamble, we summarize the provisions of the proposed regulations, summarize the related provisions in this final rule, and respond to comments received concerning each area.

It should be noted that the proposed Security Rule contained multiple proposed "requirements" and

"implementation features." In this final rule, we replace the term "requirement" with "standard." We also replace the phrase "implementation feature" with "implementation specification." We do this to maintain consistency with the use of those terms as they appear in the statute, the Transactions Rule, and the Privacy Rule. Within the comment and response portion of this final rule, for purposes of continuity, however, we use "requirement" and "implementation feature" when we are referring specifically to matters from the proposed rule. In all other instances, we use "standard" and "implementation specification."

The proposed rule would require that each covered entity (as now described in § 160.102) engaged in the electronic maintenance or transmission of health information pertaining to individuals assess potential risks and vulnerabilities to such information in its possession in electronic form, and develop, implement, and maintain appropriate security measures to protect that information. Importantly, these measures would be required to be documented and kept current.

The proposed security standard was based on three basic concepts that were derived from the Administrative Simplification provisions of HIPAA. First, the standard

should be comprehensive and coordinated to address all aspects of security. Second, it should be scalable, so that it can be effectively implemented by covered entities of all types and sizes. Third, it should not be linked to specific technologies, allowing covered entities to make use of future technology advancements.

The proposed standard consisted of four categories of requirements that a covered entity would have to address in order to safeguard the integrity, confidentiality, and availability of its electronic health information pertaining to individuals: administrative procedures, physical safeguards, technical security services, and technical mechanisms. The implementation features described the requirements in greater detail when that detail was needed. Within the four categories, the requirements and implementation features were presented in alphabetical order to convey that no one item was considered to be more important than another.

The four proposed categories of requirements and implementation features were depicted in tabular form along with the electronic signature standard in a combined matrix located at Addendum 1. We also provided a glossary of terms, at Addendum 2, to facilitate a common understanding

of the matrix entries, and at Addendum 3, we mapped available existing industry standards and guidelines to the proposed security requirements.

A. General Issues

The comment process overwhelmingly validated our basic assumptions that the entities affected by this regulation are so varied in terms of installed technology, size, resources, and relative risk, that it would be impossible to dictate a specific solution or set of solutions that would be useable by all covered entities. Many commenters also supported the concept of technological neutrality, which would afford them the flexibility to select appropriate technology solutions and to adopt new technology over time.

1. Security Rule and Privacy Rule Distinctions

As many commenters recognized, security and privacy are inextricably linked. The protection of the privacy of information depends in large part on the existence of security measures to protect that information. It is important that we note several distinct differences between the Privacy Rule and the Security Rule.

The security standards below define administrative, physical, and technical safeguards to protect the

confidentiality, integrity, and availability of electronic protected health information. The standards require covered entities to implement basic safeguards to protect electronic protected health information from unauthorized access, alteration, deletion, and transmission. The Privacy Rule, by contrast, sets standards for how protected health information should be controlled by setting forth what uses and disclosures are authorized or required and what rights patients have with respect to their health information.

As is discussed more fully below, this rule narrows the scope of the information to which the safeguards must be applied from that proposed in the proposed rule, electronic health information pertaining to individuals, to protected health information in electronic form. Thus, the scope of information covered in this rule is consistent with the Privacy Rule, which addresses privacy protections for "protected health information." However, the scope of the Security Rule is more limited than that of the Privacy Rule. The Privacy Rule applies to protected health information in any form, whereas this rule applies only to protected health information in electronic form. It is true that, under section 1173(d) of the Act, the Secretary

has authority to cover "health information," which, by statute, includes information in other than electronic form. However, because the proposed rule proposed to cover only health information in electronic form, we do not include security standards for health information in non-electronic form in this final rule.

We received a number of comments that pertained to privacy issues. These issues were considered in the development of the Privacy Rule and many of these comments were addressed in the preamble of the Privacy Rule. Therefore, we are referring the reader to that document for a discussion of those issues.

2. Level of Detail

We solicited comments as to the level of detail expressed in the required implementation features; that is, we specifically wanted to know whether commenters believe the level of detail of any proposed requirement went beyond what is necessary or appropriate. We received numerous comments expressing the view that the security standards should not be overly prescriptive because the speed with which technology is evolving could make specific requirements obsolete and might in fact deter technological progress. We have accordingly written the final rule to

frame the standards in terms that are as generic as possible and which, generally speaking, may be met through various approaches or technologies.

3. Implementation Specifications

In addition to adopting standards, this rule adopts implementation specifications that provide instructions for implementing those standards. However, in some cases, the standard itself includes all the necessary instructions for implementation. In these instances, there may be no corresponding implementation specification for the standard specifically set forth in the regulations text. In those instances, the standards themselves also serve as the implementation specification. In other words, in those instances, we are adopting one set of instructions as both the standard and the implementation specification. The implementation specification would, accordingly, in those instances be required.

In this final rule, we adopt both "required" and "addressable" implementation specifications. We introduce the concept of "addressable implementation specifications" to provide covered entities additional flexibility with respect to compliance with the security standards.

In meeting standards that contain addressable

implementation specifications, a covered entity will ultimately do one of the following: (a) implement one or more of the addressable implementation specifications; (b) implement one or more alternative security measures; (c) implement a combination of both; or (d) not implement either an addressable implementation specification or an alternative security measure. In all cases, the covered entity must meet the standards, as explained below.

The entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. Based upon this decision the following applies:

(a) If a given addressable implementation specification is determined to be reasonable and appropriate, the covered entity must implement it.

(b) If a given addressable implementation specification is determined to be an inappropriate and/or unreasonable security measure for the covered entity, but the standard cannot be met without implementation of an

additional security safeguard, the covered entity may implement an alternate measure that accomplishes the same end as the addressable implementation specification. An entity that meets a given standard through alternative measures must document the decision not to implement the addressable implementation specification, the rationale behind that decision, and the alternative safeguard implemented to meet the standard. For example, the addressable implementation specification for the integrity standard calls for electronic mechanisms to corroborate that data have not been altered or destroyed in an unauthorized manner (see 45 CFR 164.312 (c)(2)). In a small provider's office environment, it might well be unreasonable and inappropriate to make electronic copies of the data in question. Rather, it might well be more practical and afford a sufficient safeguard to make paper copies of the data.

(c) A covered entity may also decide that a given implementation specification is simply not applicable (that is, neither reasonable nor appropriate) to its situation and that the standard can be met without implementation of an alternative measure in place of the addressable implementation specification. In this scenario, the

covered entity must document the decision not to implement the addressable specification, the rationale behind that decision, and how the standard is being met. For example, under the information access management standard, an access establishment and modification implementation specification reads: "implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process" (45 CFR 164.308(a)(4)(ii)(c)). It is possible that a small practice, with one or more individuals equally responsible for establishing and maintaining all automated patient records, will not need to establish policies and procedures for granting access to that electronic protected health information because the access rights are equal for all of the individuals.

a. Comment: A large number of commenters indicated that mandating 69 implementation features would result in a regulation that is too burdensome, intrusive, and difficult to implement. These commenters requested that the implementation features be made optional to meet the requirements. A number of other commenters requested that all implementation features be removed from the regulation.

Response: Deleting the implementation specifications would result in the standards being too general to understand, apply effectively, and enforce consistently. Moreover, a number of implementation specifications are so basic that no covered entity could effectively protect electronic protected health information without implementing them. We selected 13 of these mandatory implementation specifications based on (1) the expertise of Federal security experts and generally accepted industry practices and, (2) the recommendation for immediate implementation of certain technical and organizational practices and procedures described in Chapter 6 of For The Record: Protecting Electronic Health Information, a 1997 report by the National Research Council (NRC). These mandatory implementation specifications are referred to as required implementation specifications and are reflected in the NRC report's recommendations. Risk Analysis and Risk management are found in the NRC recommendation title System Assessment; Sanction Policy is required in the Sanctions recommendation; Information system Activity Review is discussed in Audit Trails; Response and Reporting circumstances.

In addition, a number of voluntary national and regional organizations have been formed to address HIPAA implementation issues and to facilitate communication among trading partners. These include the Strategic National Implementation Process (SNIP) developed under the auspices of the Workgroup for Electronic Data Interchange (WEDI), an organization named in the HIPAA statute to consult with the Secretary of HHS on HIPAA issues. Some of these organizations have developed white papers, tools, and recommended best practices addressing a number of HIPAA issues, including security. Covered entities may wish to examine these products to determine if they are relevant and useful in their own implementation efforts. A partial list of these organizations can be found at http://www.snip.wedo.org. We believe that these and other future industry-developed guidelines and/or models may provide valuable assistance to covered entities implementing these standards but must caution that HHS does not rate or endorse any such guidelines and/or models and the value of its content must be determine by the user.

b. Comment: Many commenters asked us to develop guidelines and models to aid in complying with the Security Rule. Several commenters either offered to participate in

the development of guidelines and models or suggested entities that should be invited to participate.

Response: We agree that creation of compliance tools and guidelines for different business environments could assist covered entities to implement the HIPAA Security Rule. We plan to issue guidance documents after the publication of this final rule. However, it is critical for each covered entity to establish policies and procedures that address its own unique risks and circumstances.

In addition, a number of voluntary national and regional organizations have been formed to address HIPAA implementation issues and to facilitate communication among trading partners. These include the Strategic National Implementation Process (SNIP) developed under the auspices of the Workgroup for Electronic Data Interchange (WEDI), an organization named in the HIPAA statute to consult with the Secretary of HHS on HIPAA issues. Some of these organizations have developed white papers, tools, and recommended best practices addressing a number of HIPAA issues, including security. Covered entities may wish to examine these products to determine if they are relevant and useful in their own implementation efforts. A partial

list of these organizations can be found at http://www.snip.wedi.org. We believe that these and other future industry-developed guidelines and/or models may provide valuable assistance to covered entities implementing these standards but must caution that HHS does not rate or endorse any such guidelines and/or models and the value of its content must be determined by the user.

4. Examples

Comment: We received a number of comments that demonstrated confusion regarding the purpose of the examples of security solutions that were included throughout the proposed rule. Commenters stated that they could not, or did not wish to, adopt various security measures suggested in examples. Other commenters asked that we include additional options within the examples. Some commenters referred specifically to the example provided in the proposed rule demonstrating how a small or rural provider might comply with the standards. One commenter asked for clarification that the examples are not mandatory measures that are required to demonstrate compliance, but are merely meant as a guide when implementing the security standards. Another commenter expressed support for the use of examples to clarify the

intent of text descriptions.

Response: We wish to clarify that examples are used only as illustrations of possible approaches, and are included to serve as a springboard for ideas. The steps that a covered entity will actually need to take to comply with these regulations will be dependent upon its own particular environment and circumstances and risk assessment. The examples do not describe mandatory measures, nor do they represent the only, or even the best, way of achieving compliance. The most appropriate means of compliance for any covered entity can only be determined by that entity assessing its own risks and deciding upon the measures that would best mitigate those risks.

B. Applicability (§ 164.302)

We proposed that the security standards would apply to health plans, health care clearinghouses, and to health care providers that maintain or transmit health information electronically. The proposed security standards would apply to all electronic health information maintained or transmitted, regardless of format (standard transaction or a proprietary format). No distinction would be made between internal corporate entity communication or communication external to the corporate entity. Electronic

transmissions would include transactions using all media, even when the information is physically moved from one location to another using magnetic tape, disk, or other machine readable media. Transmissions over the Internet (wide-open), extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks would be included. We proposed that telephone voice response and "faxback" systems (a request for information made via voice using a fax machine and requested information returned via that same machine as a fax) would not be included but we solicited comments on this proposed exclusion.

This final rule simplifies the applicability statement greatly. Section 164.302 provides that the security standards apply to covered entities; the scope of the information covered is specified in § 164.306 (see the discussion under that section below regarding the changes and revisions to the scope of information covered).

1. Comment: A number of commenters requested clarification of who must comply with the standards. The preamble and proposed § 142.102 and § 142.302 stated: "Each person described in section 1172(a) of the Act who

maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards." Commenters suggested that this statement is in conflict with the law, which defines a covered entity as a health plan, a clearinghouse, or a health care provider that conducts certain transactions electronically. The commentors apparently did not realize that section 1172(a) of the Act contains the definition of covered entities.

Response: Section 164.302 below makes the security standards applicable to "covered entities." The term "covered entity" is defined at § 160.103 as one of the following: (1) a health plan; (2) a health care clearinghouse; (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by part 162 of title 45 of the Code of Federal Regulations (CFR). The rationale for the use and the meaning of the term "covered entity" is discussed in the preamble to the Privacy Rule (65 FR 82476 through 82477). As that discussion makes clear, the standards only apply to health care providers who engage electronically in the transactions for which standards have been adopted.

2. Comment: Several commenters recommended expansion of applicability, either to other specific entities, or to all entities involved in health care. Others wanted to know whether the standards apply to entities such as employers, public health organizations, medical schools, universities, research organizations, plan brokers, or non-EDI providers. One commenter asked whether the standards apply to State data organizations operating in capacities other than as plans, clearinghouses, or providers. Still other commenters stated that it was inappropriate to include physicians and other health care professionals in the same category as plans and clearinghouses, arguing that providers should be subject to different, less burdensome requirements because they already protect health information.

Response: The statute does not cover all health care entities that transmit or maintain individually identifiable health information. Section 1172(a) of the Act provides that only health plans, health care clearinghouses, and certain health care providers (as discussed above) are covered. With respect to the comments regarding the difference between providers and plans/clearinghouses, we have structured the Security Rule

to be scalable and flexible enough to allow different entities to implement the standards in a manner that is appropriate for their circumstances. Regarding the coverage of entities not within the jurisdiction of HIPAA, see the Privacy Rule at 82567 through 82571.

3. Comment: One commenter asked whether the standards would apply to research organizations, both to those affiliated with health care providers and those that are not.

Response: Only health plans, health care clearinghouses, and certain health care providers are required to comply with the security standards. Researchers who are members of a covered entity's work force may be covered by the security standards as part of the covered entity. See the definition of "workforce" at 45 CFR 160.103. Note, however, that a covered entity could, under appropriate circumstances, exclude a researcher or research division from its health care component or components (see § 164.105(a)). Researchers who are not part of the covered entity's workforce and are not themselves covered entities are not subject to the standards.

4. Comment: Several commenters stated that internal networks and external networks should be treated differently. One commenter asked for further clarification of the difference between what needs to be secured external to a corporation versus the security of data movement within an organization. Another stated that complying with the security standards for internal communications may prove difficult and costly to monitor and control. In contrast, one commenter stated that the existence of requirements should not depend on whether use of information is for internal or external purposes.

Another commenter argued that the regulation goes beyond the intent of the law, and while communication of electronic information between entities should be covered, the law was never intended to mandate changes to an entity's internal automated systems. One commenter requested that raw data that are only for the internal use of a facility be excluded, provided that reasonable safeguards are in place to keep the raw data under the control of the facility.

Response: Section 1173(d)(2) of the Act states:

> Each person described in section 1172(a) who maintains or transmits health information shall

> maintain reasonable and appropriate administrative, technical, and physical safeguards--(A) to ensure the integrity and confidentiality of the information; (B) to protect against any reasonably anticipated--(i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information; and (C) otherwise to ensure compliance with this part by the officers and employees of such person.

This language draws no distinction between internal and external data movement. Therefore, this final rule covers electronic protected health information at rest (that is, in storage) as well as during transmission. Appropriate protections must be applied, regardless of whether the data are at rest or being transmitted. However, because each entity's security needs are unique, the specific protections determined appropriate to adequately protect information will vary and will be determined by each entity in complying with the standards (see the discussion below).

5. Comment: Several commenters found the following statement in the proposed rule (63 FR 43245) at section

II.A. confusing and asked for clarification: "With the exception of the security standard, transmission within a corporate entity would not be required to comply with the standards."

Response: In the final Transactions Rule, we revised our approach concerning the transaction and code set exemptions, replacing this concept with other tests that determine whether a particular transaction is subject to those standards (see the discussion in the Transactions Rule at 65 FR 50316 through 50318). We also note that the Privacy Rule regulates a covered entity's use, as well as disclosure, of protected health information.

6. Comment: One commenter stated that research would be hampered if proposed § 142.306(a) applied. The commenter believes that research uses of health information should be excluded or the standard should be revised to allow appropriate flexibility for research depending on the risk to patients or subjects (for example, if the information is anonymous, there is no risk, and it would not be necessary to meet the security standards).

Response: If electronic protected health information is de-identified (as truly anonymous information would be), it is not covered by this rule because it is no longer

electronic protected health information (see 45 CFR 164.502(d) and 164.514(a)). Electronic protected health information received, created, or maintained by a covered entity, or that is transmitted by covered entities, is covered by the security standards and must be protected. To the extent a researcher is a covered entity, the researcher must comply with these standards with respect to electronic protected health information. Otherwise, the conditions for release of such information to researchers is governed by the Privacy Rule. See, for example, 45 CFR 164.512(i), 164.514(e) and 164.502(d). These standards would not apply to the researchers as such in the latter circumstances.

7. Comment: One commenter asked to what extent individual patients are subject to the standards. For example, some telemedicine practices support the use of diagnostic systems in the patient's home, which can be used to conduct tests and send results to a remote physician. In other cases, patients may be responsible for the filing of insurance claims directly and will need the ability to verify facts, confirm receipt of claims, and so on. The commenter asked if it is the intent of the rule to include electronic transmission to or from the patient.

Response: Patients are not covered entities and, thus, are not subject to these standards. With respect to transmissions from covered entities, covered entities must protect electronic protected health information when they transmit that information. See also the discussion of encryption in section III.G.

C. Transition to the Final Rule

The proposed rule included definitions for a number of terms that have now already been promulgated as part of the Transactions Rule or the Privacy Rule. Comments related to the definitions of "code set," "health care clearinghouse," "health plan," "health care provider," "small health plan," "standard" and "transaction," are addressed in the Transactions Rule at 65 FR 50319 through 50320. Comments concerning the definition of "individually identifiable health information" are discussed below, but are also addressed in the Privacy Rule at 65 FR 82611 through 82613. In addition, a few terms were redefined in the final Standards for Privacy of Individually Identifiable Health Information (67 FR 53182), issued on August 14, 2002 (Privacy Modifications). Certain terms that were defined in the proposed rule are not used in the final rule because they are no longer necessary. Other terms defined in the

proposed rule are defined within the explanation of the standards in the final rule and are discussed in the preamble discussions in § 164.308 through § 164.312.

Definitions of terms relevant to the security standards now appear in the regulations text provisions as indicated below:

§ 160.103: Definitions of the following terms relevant to this rule appear in § 160.103: "business associate," "covered entity," "disclosure," "electronic media," "electronic protected health information," health care," "health care clearinghouse," "health care provider," "health information," "health plan," "individual," "individually identifiable health information," "implementation specification," "organized health care arrangement," "protected health information," "standard," "use," and "workforce." These terms were discussed in connection with the Transaction and Privacy Rules and with the exception of the terms "covered entity", "disclosure" "electronic protected health information", "health information," "individual," "organized health care arrangement," "protected health information," and "use," we will not discuss them in this document. We note that the

definition of those terms are not changed in the final rule.

§ 162.103: We have moved the definition of "electronic media" at § 162.103 to § 160.103 and have modified it to clarify that the term includes storage of information. The term "electronic media" is used in the definition of "protected health information." Both the privacy and security standards apply to information "at rest" as well as to information being transmitted.

We note that we have deleted the reference to § 162.103 in paragraph (1)(ii) of the definition of "protected health information," since both definitions, "electronic media" and "protected health information," have been moved to this section. Also, it is unnecessary, because the definitions of § 160.103 apply to all of the rule in parts 160, 162, and 164.

We have also clarified that the physical movement of electronic media from place to place is not limited to magnetic tape, disk, or compact disk. This clarification removes a restriction as to what is considered to be physical electronic media, thereby allowing for future technological innovation. We further clarified that transmission of information not in electronic form before

the transmission, for example, paper or voice, is not covered by this definition.

§ 164.103: The following term "plan sponsor" now appears in the new § 164.103, which consists of definitions of terms common to both subpart C and subpart E (the privacy standards). This definition was moved, without substantive change, from § 164.501 and has the meaning given to it in that section, and comments relating to this definitions are discussed in connection with that section in the Privacy Rule at 65 FR 82607, 82611 through 82613, 82618 through 82622, and 82629.

§ 164.304: Definitions specifically applicable to the Security Rule appear in § 164.304, and these are discussed below. These definitions are from, or derived from, currently accepted definitions in industry publications, such as, the International Organization for Standards (ISO) 7498-2 and the American Society for Testing and Materials (ASTM) E1762-95.

The following terms in § 164.304 are taken from the proposed rule text or the glossary in Addendum 2 of the proposed rule (63 FR 43271), were not commented on, and/or are unchanged or have only minor technical changes for purposes of clarification and are not discussed below:

"access," "authentication," "availability," confidentiality," "encryption," "password," and "security."

§ 164.314: Four terms were defined in § 164.504(a) of the Privacy Rule ("common control," "common ownership," "health care component," and "hybrid entity"). Because these terms apply to both security and privacy, their definitions have been moved to § 164.103 without change. Those terms are discussed in the Privacy Rule at 65 FR 82502 through 82503 and at 67 FR 53203 through 53207.

1. Covered Entity (§ 160.103)

Comment: One commenter asked if transcription services were covered entities. The question arose because transcription is often the first electronic or printed source of clinical information. Concern was expressed about the application of physical safeguard standards to the transcribers working for transcription companies or health care providers, either as employees or as independent contractors.

Another commenter expressed concern that scalability was limited to only small providers. The commenter explained that Third Party Administrators (TPAs) allow claim processors to work at home. Some TPAs have noted that it would be impossible to comply with the security

standards for home-based claims processors.

Response: A covered entity's responsibility to implement security standards extends to the members of its workforce, whether they work at home or on-site. Because a covered entity is responsible for ensuring the security of the information in its care, the covered entity must include "at home" functions in its security process. While an independent transcription company or a TPA may not be covered entities, they will be a business associate of the covered entity because their activities fall under paragraph (1)(i)(a) of the definition of that term. For business associate provisions see proposed preamble section III.E.8. and § 164.308(b)(1) and § 164.314(c) of this final rule.

2. Health Care and Medical Care (§ 160.103)

Comment: One commenter asked whether "medical care," which is defined in the proposed rule, and "health care," which is not, are synonymous.

Response: The term "medical care," as used in the proposed rule (63 FR 43242), was intended to be synonymous with "health care." The term "medical care" is not included in this final rule. It is, however, included in the definition of "health plan," where its meaning is not

synonymous with "health care." For a full discussion of this issue and its resolution, see the Privacy Rule (65 FR 82578).

3. Health Information and Individually Identifiable Health Information (§ 160.103)

We note that the definitions of "health information" and "individually identifiable health information" remain unchanged from those published in the Transactions and Privacy Rules.

a. Comment: A number of commenters asked that the definition of "health information" be expanded to include information collected by additional entities. Several commenters wanted the definition to include health information collected, maintained, or transmitted by any entity, and one commenter suggested the inclusion of aggregated information not identifiable to an individual. Several commenters asked that eligibility information be excluded from the definition of health information. Several commenters wanted the definition broadened to include demographics.

Response: Our definition of health information is taken from the definition in section 1171(4) of the Act, which provides that health information relates to the

health or condition of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual. The statutory definition also specifies the entities by which health information is created or received. We note that, because "individually identifiable health information" is a subset of "health information" and by statute includes demographic information, "health information" necessarily includes demographic information. We think this is clear as a matter of statutory construction and does not require further regulatory change.

b. Comment: Several commenters asked that we clarify the difference between "health information" and "individually identifiable" and "health information pertaining to an individual" as used in the August 12, 1998 proposed rule (63 FR 43242). Additionally, commenters asked that we be more consistent in the use of these terms and recommended use of the term "individually identifiable health information."

Two commenters stated that it is important to distinguish between "health information pertaining to an individual" and "individually identifiable health information," as in reporting statistics at various levels

there will always be a need to bring forth information pertaining to an individual.

One commenter recommended that the standards apply only to individually identifiable health information. Another stated that in § 142.306(b) of the proposed rule, "health information pertaining to an individual" should be changed to "individually identifiable health information," as nonidentifiable information can be used for utilization review and other purposes. As written, the regulation text could limit the ability to use data, for example, from a clearinghouse for compliance monitoring.

Response: In general, we agree with these commenters, and note that these comments are largely mooted by the decision, reflected in § 164.306 below and discussed in section III.D.1. of this final rule, to cover only electronic protected health information in this final rule.

c. Comment: Several commenters stated that the definition of "individually identifiable health information" is not in the regulations and should be added.

Response: We note that the definition of "individually identifiable health information" appears at § 160.103, which applies to this final rule.

4. Protected Health Information (§ 160.103)

This term is moved from § 164.501 to § 160.103 because it applies to both subparts C (security) and E (privacy). See 67 FR 53192 through 531936 regarding the definition of "protected health information."

Also, the term "electronic media" is included in paragraphs (1)(i) and (ii) of the definition of "protected health information," as specified in this section.

In addition, we added the definitions of "covered functions," "plan sponsor," and "Required by law" to § 164.103.

5. Breach (§ 164.304)

Comment: One commenter asked that "breach" be defined.

Response: The term "breach" has been deleted and therefore not defined. Instead, we define the term "security incident," which better describes the types of situations we were referring to as breaches.

6. Facility (§ 164.304)

This new term has been added as a result of changing the name of the "physical access control" standard to "facility access control." This change was made based on comments indicating that the original term was not

descriptive. We have defined the term "facility" as the physical premises and interior and exterior of a building.

7. Security Incident (§ 164.304)

Comment: We received comments asking that this term be defined.

Response: This final rule defines "Security incident" in § 164.304 as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

8. System (§ 164.304)

Comment: One commenter asked that "system" be defined.

Response: This final rule defines "system," in the context of an information system, in § 164.304 as "an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people."

9. Workstation (§ 164.304)

Comment: One commenter expressed concern that the use of the term "workstation" implied limited applicability to

fixed devices (such as terminals), excluding laptops and other portable devices.

Response: We have added a definition of the term "workstation" to clarify that portable devices are also included. This final rule defines workstation as "an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment."

10. Definitions Not Adopted

Several definitions in the proposed regulations text and glossary are not adopted as definitions in the final rule: "participant," "contingency plan," "risk," "role-based access control," and "user-based access control." The terms "participant," "role-based access control," and "user-based access control" are not used in this final rule and thus are not defined. "Risk" is not defined as its meaning is generally understood. While we do not define the term, we address "contingency plan" as a standard in § 164.308(a)(7) below.

a. Comment: We received comments requesting that we define the following terms: "token" and "documentation."

Response: These terms were defined in Addendum 2 of the proposed rule. In this final rule, we do not adopt a definition for "token" because it is not used in the final rule. "Documentation" is discussed in § 164.316 below.

b. Comment: We received several comments that "small" and "rural" should be defined as those terms apply to providers. We received an equal number of comments stating that there is no need to define these terms. One commenter stated that definitions for these terms would be necessary only if special exemptions existed for small and rural providers. Several commenters suggested initiation of a study to determine limitations and potential barriers small and rural providers will have in implementing these regulations.

Response: The statute requires that we address the needs of small and rural providers. We believe that we have done this through the provisions, which require the risk assessment and the response to be assessment based on the needs and capabilities of the entity. This scalability concept takes the needs of those providers into account and eliminates any need to define those terms.

c. Comment: In the proposed rule, we proposed the following definition for the term "Access control": "A

method of restricting access to resources, allowing only privileged entities access. Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, classification, and subject-object separation." One commenter believed the proposed definition is too restrictive and requested revision of the definition to read: "Access control refers to a method of restricting access to resources, allowing access to only those entities which have been specifically granted the desired access rights." Another commenter wanted the definition expanded to include partitioned rule-based access control (PRBAC).

Response: We agree with the commenter who suggested that the definition as proposed seemed too restrictive. In this case, as in many others, a number of commenters believed the examples given in the proposed rule provided the only acceptable compliance actions. As previously noted, in order to clarify that the examples listed were not to be considered all-inclusive, we have generalized the proposed requirements in this final rule. In this case, we have also generalized the requirements and placed the substantive provisions governing access control at § 164.308(a)(4), § 164.310(a)(1), and § 164.312(a)(1).

With respect to PRBAC, the access control standard does not exclude this control, and entities should adopt it if appropriate to their circumstances.

D. General Rules (§ 164.306)

In the proposed rule, we proposed to cover all health information maintained or transmitted in electronic form by a covered entity. We proposed to adopt, in § 142.308, a nation-wide security standard that would require covered entities to implement security measures that would be technology-neutral and scalable, and yet integrate all the components of security (administrative procedures, physical safeguards, technical security services, and technical security mechanisms) that must be in place to preserve health information confidentiality, integrity, and availability (three basic elements of security). Since no comprehensive, scalable, and technology-neutral set of standards currently exists, we proposed to designate a new standard, which would define the security requirements to be fulfilled.

The proposed rule proposed to define the security standard as a set of scalable, technology-neutral requirements with implementation features that providers, plans, and clearinghouses would have to include in their

operations to ensure that health information pertaining to an individual that is electronically maintained or electronically transmitted remains safeguarded. The proposed rule would have required that each affected entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its own unique security needs. How individual security requirements would be satisfied and which technology to use would be business decisions that each entity would have to make.

In the final rule we adopt this basic framework. In § 164.306, we set forth general rules pertaining to the security standards. In paragraph (a), we describe the general requirements. Paragraph (a) generally reflects section 1173(d)(2) of the Act, but makes explicit the connection between the security standards and the privacy standards (see § 164.306(a)(3)). In § 164.306(a)(1), we provide that the security standards apply to all electronic protected health information the covered entity creates, receives, maintains, or transmits. In paragraph (b)(1), we provide explicitly for the scalability of this rule by discussing the flexibility of the standards, and paragraph (b)(2) of § 164.306 discusses various factors covered

entities must consider in complying with the standards.

The provisions of § 164.306(c) provide the framework for the security standards, and establish the requirement that covered entities must comply with the standards. The administrative, physical, and technical safeguards a covered entity employs must be reasonable and appropriate to accomplish the tasks outlined in paragraphs (1) through (4) of § 164.306(a). Thus, an entity's risk analysis and risk management measures required by § 164.308(a)(1) must be designed to lead to the implementation of security measures that will comply with § 164.306(a).

It should be noted that the implementation of reasonable and appropriate security measures also supports compliance with the privacy standards, just as the lack of adequate security can increase the risk of violation of the privacy standards. If, for example, a particular safeguard is inadequate because it routinely permits reasonably anticipated uses or disclosures of electronic protected health information that are not permitted by the Privacy Rule, and that could have been prevented by implementation of one or more security measures appropriate to the scale of the covered entity, the covered entity would not only be violating the Privacy Rule, but would also not be in

compliance with § 164.306(a)(3) of this rule.

Paragraph (d) of § 164.306 establishes two types of implementation specifications, required and addressable. It provides that required implementation specifications must be met. However, with respect to implementation specifications that are addressable, § 164.306(d)(3) specifies that covered entities must assess whether an implementation specification is a reasonable and appropriate safeguard in its environment, which may include consideration of factors such as the size and capability of the organization as well as the risk. If the organization determines it is a reasonable and appropriate safeguard, it must implement the specification. If an addressable implementation specification is determined not to be a reasonable and appropriate answer to a covered entity's security needs, the covered entity must do one of two things: implement another equivalent measure if reasonable and appropriate; or if the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure at all. The covered entity must document the rationale behind not implementing the implementation specification. See the detailed discussion in section

II.A.3.

Paragraph (e) of § 164.306 addresses the requirement for covered entities to maintain the security measures implemented by reviewing and modifying the measures as needed to continue the provision of reasonable and appropriate protections, for example, as technology moves forward, and as new threats or vulnerabilities are discovered.

1. Scope of Health Information Covered by the Rule (§ 164.306(a))

We proposed to cover health information maintained or transmitted by a covered entity in electronic form. We have modified, by narrowing, the scope of health information to be safeguarded under this rule from that which was proposed. The statute requires the privacy standards to cover individually identifiable health information. The Privacy Rule covers all individually identifiable information except for: (1) education records covered by the Family and Educational Rights and Privacy Act (FERPA); (2) records described in 20 U.S.C. 1232g(a)(4)(B)(iv); and (3) employment records. (see the Privacy Rule at 65 FR 82496. See also 67 FR 53191 through 53193). The scope of information covered in the

Privacy Rule is referred to as "protected health information." Based upon the comments we received, we align the requirements of the Security and Privacy Rules with regard to the scope of information covered, in order to eliminate confusion and ease implementation. Thus, this final rule requires protection of the same scope of information as that covered by the Privacy Rule, except that it only covers that information if it is in electronic form.

We note that standards for the security of all health information or protected health information in nonelectronic form may be proposed at a later date.

a. Comment: One commenter stated that the rule should apply to aggregate information that is not identifiable to an individual. In contrast, another commenter asked that health information used for statistical analysis be exempted if the covered entity may reasonably expect that the removed information cannot be used to re-identify an individual.

Response: As a general proposition, any electronic protected health information received, created, maintained, or transmitted by a covered entity is covered by this final rule. We agree with the second commenter that certain

information, from which identifiers have been stripped, does not come within the purview of this final rule. Information that is de-identified, as defined in the Privacy Rule at § 164.502(d) and § 164.514(a), is not "individually identifiable" within the meaning of these rules and, thus, does not come within the definition of "protected health information." It accordingly is not covered by this final rule. For a full discussion of the issues of de-identification and re-identification of individually identifiable health information see 65 FR 82499 and 82708 through 82712 and 67 FR 53232 through 53234.

b. Comment: Several commenters asked whether systems that determine eligibility of clients for insurance coverage under broad categories such as medical coverage groups are considered health information. One commenter asked that we specifically exclude eligibility information from the standards.

Response: We cannot accept the latter suggestion. Eligibility information will typically be individually identifiable, and much eligibility information will also contain health information. If the information is "individually identifiable" and is "health information,"

(with three very specific exceptions noted in the general discussion above) and it is in electronic form, it is covered by the security standards if maintained or transmitted by a covered entity.

c. Comment: Several commenters requested clarification as to whether the standards apply to identifiable health information in paper form. Some commenters believed the rule should be applicable to paper; others argued that it should apply to all confidential, identifiable health information.

Response: While we agree that protected health information in paper or other form also should have appropriate security protections, the proposed rule proposing the security standards proposed to apply those standards to health information in electronic form only. We are, accordingly, not extending the scope in this final rule.

We may establish standards to secure protected health information in other media in a future rule, in accordance with our statutory authority to do so. See discussion, supra, responding to a comment on the definition of "health information" and "individually identifiable health information."

d. Comment: The proposed rule would have excluded "telephone voice response" and "faxback" systems from the security standards, and we specifically solicited comments on that issue. A number of commenters agreed that telephone voice response and faxback should be excluded from the regulation, suggesting that the privacy standards rather than the security standards should apply. Others wanted those systems included, on the grounds that inclusion is necessary for consistency and in keeping with the intent of the Act. Still others specifically wanted personal computer-fax transmissions included. One commenter asked for clarification of when we would cover faxes, and another commenter asked why we were excluding them. Several commenters suggested that the other security requirements provide for adequate security of these systems.

Response: In light of these comments, we have decided that telephone voice response and "faxback" (that is, a request for information from a computer made via voice or telephone keypad input with the requested information returned as a fax) systems fall under this rule because they are used as input and output devices for computers, not because they have computers in them. Excluding these

features would provide a huge loophole in any system concerned with security of the information contained and/or processed therein. It should be noted that employment of telephone voice response and/or faxback systems will generally require security protection by only one of the parties involved, and not the other. Information being transmitted via a telephone (either by voice or a DTMP tone pad) is not in electronic form (as defined in the first paragraph of the definition of "electronic media") before transmission and therefore is not subject to the Security Rule. Information being returned via a telephone voice response system in response to a telephone request is data that is already in electronic form and stored in a computer. This latter transmission does require protection under the Security Rule.

Although most recently made electronic devices contain microprocessors (a form of computer) controlled by firmware (an unchangeable form of computer program), we intend the term "computer" to include only software programmable computers, for example, personal computers, minicomputers, and mainframes. Copy machines, fax machines, and telephones, even those that contain memory and can produce multiple copies for multiple people are not intended to be

included in the term "computer." Therefore, because "paper-to-paper" faxes, person-to-person telephone calls, video teleconferencing, or messages left on voice-mail were not in electronic form before the transmission, those activities are not covered by this rule. See also the definition of "electronic media" at § 160.103.

We note that this guidance differs from the guidance regarding the applicability of the Transactions Rule to faxback and voice response systems. HHS has stated that faxback and voice response systems are not required to follow the standards mandated in the Transactions Rule. This new guidance refers only to this rule.

e. Comment: One commenter asked whether there is a need to implement special security practices to address the shipping and receiving of health information and asked that we more fully explain our expectations and solutions in the final rules.

Response: If the handling of electronic protected health information involves shipping and receiving, appropriate measures must be taken to protect the information. However, specific solutions are not provided within this rule, as discussed in section III.A.3 of this final rule. The device and media controls standard under

§ 164.310(d)(1) addresses this situation.

f. Comment: One commenter wanted the "HTML" statement reworded to eliminate a specific exemption for HTML from the regulation.

Response: The Transactions Rule did not adopt the proposed exemption for HTML. The use of HTML or any other electronic protocol is not exempt from the security standards. Generally, if protected health information is contained in any form of electronic transmission, it must be appropriately safeguarded.

g. Comment: One commenter asked to what degree "family history" is considered health information under this rule and what protections apply to family members included in a patient's family history.

Response: Any health-related "family history" contained in a patient's record that identifies a patient, including a person other than the patient, is individually identifiable health information and, to the extent it is also electronic protected health information, must be afforded the security protections.

h. Comment: Two commenters asked that the rule prohibit re-identification of de-identified data. In contrast, several commenters asked that we identify a

minimum list or threshold of specific re-identification data elements (for example, name, city, and ZIP) that would fall under this final rule so that, for example, the rule would not affect numerous systems, for example, network adequacy and population-based clinical analysis databases. One commenter asked that we establish a means to use re-identified information if the entity already has access to the information or is authorized to have access.

Response: The issue of re-identification is addressed in the Privacy Rule at § 164.502(d) and § 164.514(c). The reader is referred to those sections and the related discussion in the preamble to the Privacy Rule (65 FR 82712) and the preamble to the Privacy Modifications (67 FR 53232 through 53234) for a full discussion of the issues of re-identification. We note that once information in the possession (or constructive possession) of a covered entity is re-identified and meets the definition of electronic protected health information, the security standards apply.

2. Technology-Neutral Standards

Comment: Many commenters expressed support for our efforts to develop standards for the security of health information. A number of comments were made in support of

the technology-neutral approach of the proposed rule. For example, one commenter stated, "By avoiding prescription of the specific technologies health care entities should use to meet the law's requirements, you are opening the door for industry to apply innovation. Technologies that don't currently exist or are impractical today could, in the near future, enhance health information security while minimizing the overall cost." Several other commenters stated that the requirements should be general enough to withstand changes to technology without becoming obsolete. One commenter anticipates no problems with meeting the standards.

In contrast, one commenter suggested that whenever possible, specific technology recommendations should provide sufficient detail to promote systems interoperability and decrease the tendency toward adoption of multiple divergent standards. Several commenters stated that by letting each organization determine its own rules, the rules impose procedural burdens without any substantive benefit to security.

Response: The overwhelming majority of comments supported our position. We do not believe it is appropriate to make the standards technology-specific

because technology is simply moving too fast, for example, the increased use and sophistication of internet-enabled hand held devices. We believe that the implementation of these rules will promote the security of electronic protected health information by (1) providing integrity and confidentiality; (2) allowing only authorized individuals access to that information; and (3) ensuring its availability to those authorized to access the information. The standards do not allow organizations to make their own rules, only their own technology choices.

3. Miscellaneous Comments

a. Comment: Some commenters stated that the requirements and implementation features set out in the proposed rule were not specific enough to be considered standards, and that the actual standards are delegated to the discretion of the covered entities, at the expense of medical record privacy. Several commenters stated that it was inappropriate to balance the interests of those seeking to use identifiable medical information without patient consent against the interest of patients. Several other commenters believe that allowing covered entities to make their own decisions about the adequacy and balance of security measures undermined patient confidentiality

interests, and stated that the proposed rule did not appear to adequately consider patient concerns and viewpoints.

Response: Again, the overwhelming majority of commenters supported our approach. This final rule sets forth requirements with which covered entities must comply and labels those requirements as standards and implementation specifications. Adequate implementation of this final rule by covered entities will ensure that the electronic protected health information in a covered entity's care will be as protected as is feasible for that entity.

We disagree that covered entities are given complete discretion to determine their security polices under this rule, resulting in effect, in no standards. While cost is one factor a covered identity may consider in determining whether to implement a particular implementation specifications, there is nonetheless a clear requirement that adequate security measures be implemented, see 45 CFR 164.306(b). Cost is not meant to free covered entities from this responsibility.

b. Comment: Several commenters requested we withdraw the regulations, citing resource shortages due to Y2K preparation, upcoming privacy legislation, and/or the

"excessive micro-management" contained in the rules. One commenter stated that, to insurers, these rules were onerous, not necessary, and not justified as cost-effective, as they already have effective practices for computer security and are subject to rigorous State laws for the safeguarding of health information. Another commenter stated that these rules would adversely affect a provider's practice environment.

Response: The HIPAA statute requires us to promulgate a rule adopting security standards for health information. Resource concerns due to Y2K should no longer be an issue. Covered entities will have 2 years (or, in the case of small health plans, 3 years) from the adoption of this final rule in which to comply. Concerns relative to effective and compliance dates and the Privacy Rule are discussed under § 164.318, Compliance dates for initial implementation, below and at 65 FR 82751 through 82752.

We disagree that these standards will adversely affect a provider's practice environment. The scalability of the standards allows each covered entity to implement security protections that are appropriate to its specific needs, risks, and environments. These protections are necessary to maintain the confidentiality, integrity, and

availability of patient data. A covered entity that lacks adequate protections risks inadvertent disclosure of patient data, with resulting loss of public trust, and potential legal action. For example, a covered entity with poor facility access controls and procedures would be susceptible to hacking of its databases. A provider with appropriate security protections already in place would only need to ensure that the protections are documented and are reassessed periodically to ensure that they continue to be appropriate and are actually being implemented. Our decision to classify many implementation specifications as addressable, rather than mandatory, provides even more flexibility to covered entities to develop cost-effective solutions. We believe that insurers who already have effective security programs in place will have met many of the requirements of this regulation.

c. Comment: One commenter believes the rule is arbitrary and capricious in its requirements without any justification that they will significantly improve the security of medical records and with the likelihood that their implementation may actually increase the vulnerability of the data. The commenter noted that the data backup requirements increase access to data and that

security awareness training provides more information to employees.

Response: The standards are based on generally accepted security procedures, existing industry standards and guidelines, and recommendations contained in the National Research Council's 1997 report For The Record: Protecting Electronic Health Information, Chapter 6. We also consulted extensively with experts in the field of security throughout the health care industry. The standards are consistent with generally accepted security principles and practices that are already in widespread use.

Data backup need not result in increased access to that data. Backups should be stored in a secure location with controlled access. The appropriate secure location and access control will vary, based upon the security needs of the covered entity. For example, a procedure as simple as locking backup diskettes in a safe place and restricting who has access to the key may be suitable for one entity, whereas another may need to store backed-up information off-site in a secure computer facility. The information provided in security awareness training heightens awareness of security anomalies and helps to prevent security

incidents.

d. Comment: Several commenters suggested that the proposed rule appears to reflect the Medicare program's perspective on security risks and solutions, and that it should be noted that not all industry segments share all the same risks as Medicare. One commenter stated that as future proposed rules are drafted, we should solicit input from those most significantly affected, for example, providers, plans, and clearinghouses. Others stated that Medicaid agencies were not sufficiently involved in the discussions and debate. Still another stated that States would be unable to perform some basic business functions if all the standards are not designed to meet their needs.

Response: We believe that the standards are consistent with common industry practices and equitable, and that there has been adequate consultation with interested parties in the development of the standards. These standards are the result of an intensive process of public consultation. We consulted with the National Uniform Billing Committee, the National Uniform Claim Committee, the American Dental Association, and the Workgroup for Electronic Data Interchange, in the course of developing the proposed rule. Those organizations were

specifically named in the Act to advise the Secretary, and their membership is drawn from the full spectrum of industry segments. In addition, the National Committee on Vital and Health Statistics (NCVHS), an independent advisory group to the Secretary, held numerous public hearings to obtain the views of interested parties. Again, many segments of the health care industry, including provider groups, health plans, clearinghouses, vendors, and government programs participated actively. The NCVHS developed recommendations to the Secretary, which were relied upon as we developed the proposed rule. Finally, we note that the opportunity to comment was available to all during the public comment period.

e. Comment: One commenter stated that there is a need to ensure the confidentiality of risk analysis information that may contain sensitive information.

Response: The information included in a risk analysis would not be subject to the security standards if it does not include electronic protected health information. We agree that risk analysis data could contain sensitive information, just as other business information can be sensitive. Covered entities may wish to develop their own business rules regarding access to and protections for risk

analysis data.

f. Comment: One commenter expressed concern over the statement in the preamble of the proposed rule (63 FR 43250) that read: "No one item is considered to be more important than another." The commenter suggested that security management should be viewed as most critical and perhaps what forms the foundation for all other security actions.

Response: The majority of comments received on this subject requested that we prioritize the standards. In response, we have regrouped the standards and implementation specifications in what we believe is a logical order within each of three categories: "Administrative safeguards," "Physical safeguards," and "Technical safeguards." In this final rule, we order the standards in such a way that the "Security management process" is listed first under the "Administrative safeguards" section, as we believe this forms the foundation on which all of the other standards depend. The determination of the specific security measures to be implemented to comply with the standards will, in large part, be dependent upon completion of the implementation specifications within the security management process

standard (see § 164.308(a)(1)). We emphasize, however, that an entity implementing these standards may choose to implement them in any order, as long as the standards are met.

g. Comment: One commenter stated that there is a need for requirements concerning organizational practices (for example, education, training, and security and confidentiality policies), as well as technical practices and procedures.

Response: We agree. Section 164.308 of this final rule describes administrative safeguards that address these topics. Section 164.308 requires covered entities to implement standards and required implementation specifications, as well as consider and implement, when appropriate and reasonable, addressable implementation specifications. For example, the security management process standard requires implementation of a risk analysis, risk management, a sanction policy, and an information system activity review. The information access management standard requires consideration, and implementation where appropriate and reasonable, of access authorization and access establishment and modification policies and procedures. Other areas addressed are

assigned security responsibility, workforce security, security awareness and training, security incident procedures, contingency planning, business associate contracts, and evaluation.

h. Comment: One commenter stated that internal and external security requirements should be separated and dealt with independently.

Response: The presentation of the standards within this final rule could have been structured in numerous ways, including by addressing separate internal and external security standards. We chose the current structure as we considered it a logical breakout for purposes of display within this final rule. Under our structure a covered entity may apply a given standard to internal activities and to external activities. Had we displayed separately the standards for internal security and the standards for external security, we would have needed to describe a number of the standards twice, as many apply to both internal and external security. However, a given entity may address the standards in whatever order it chooses, as long as the standards are met.

i. Comment: Two commenters stated that the standards identified in Addendum 3 of the proposed rule may not all

have matured to implementation readiness.

Response: Addendum 3 of the proposed rule cross-referred individual requirements on the matrix to existing industry standards of varying levels of maturity. Addendum 3 was intended to show what we evaluated in searching for existing industry standards that could be adopted on a national level. No one standard was found to be comprehensive enough to be adopted, and none were proposed as the standards to be met under the Security Rule.

j. Comment: One commenter suggested we include a revised preamble in the final publication. Another questioned how clarification of points in the preamble will be handled if the preamble is not part of the final regulation.

Response: Preambles to proposed rules are not republished in the final rule. The preamble in this final rule contains summaries of the information presented in the preamble of the proposed rule, summaries of the comments received during the public comment period, and responses to questions and concerns raised in those comments and a summary of changes made. Additional clarification will be provided by HHS on an ongoing basis through written

documents and postings on HHS's websites.

k. Comment: One commenter asked that we clarify that no third party can require implementation of more security features than are required in the final rule, for example, a third party could not require encryption but may choose to accept it if the other party so desires.

Response: The security standards establish a minimum level of security to be met by covered entities. It is not our intent to limit the level of security that may be agreed to between trading partners or others above this floor.

l. Comment: One commenter asked how privacy legislation would affect these rules. The commenter inquired whether covered entities will have to reassess and revise actions already taken in the spirit of compliance with the security regulations.

Response: We cannot predict if or how future legislation may affect the rules below. At present, the privacy standards at subpart E of 42 CFR part 164 have been adopted, and this final rule is compatible with them.

m. Comment: One commenter stated that a data classification policy, that is a method of assigning sensitivity ratings to specific pieces of data, should be

part of the final regulations.

Response: We did not adopt such a policy because this final rule requires a floor of protection of all electronic protected health information. A covered entity has the option to exceed this floor. The sensitivity of information, the risks to and vulnerabilities of electronic protected health information and the means that should be employed to protect it are business determinations and decisions to be made by each covered entity.

n. Comment: One commenter stated that this proposed rule conflicts with previously stated rules that acceptable "standards" must have been developed by ANSI-recognized Standards Development Organizations (SDOs).

Response: In general, HHS is required to adopt standards developed by ANSI-accredited SDOs when such standards exist. The currently existing security standards developed by ANSI-recognized SDOs are targeted to specific technologies and/or activities. No existing security standard, or group of standards, is technology-neutral, scaleable to the extent required by HIPAA, and broad enough to be adopted in this final rule. Therefore, this final rule adopts standards under section 1172(c)(2)(B) of the Act, which permits us to develop standards when no industry

standards exist.

o. Comment: One commenter stated that this regulation goes beyond the scope of the law, unjustifiably extending into business practices, employee policies, and facility security.

Response: We do not believe that this regulation goes beyond the scope of the law. The law requires HHS to adopt standards for reasonable and appropriate security safeguards concerning such matters as compliance by the officers and employees of covered entities, protection against reasonably anticipated unauthorized uses and disclosures of health information, and so on. Such standards will inevitably address the areas the commenter pointed to.

The intent of this regulation is to provide standards for the protection of electronic protected health information in accordance with the Act. In order to do this, covered entities are required to implement administrative, physical, and technical safeguards. Those entities must ensure that data are protected, to the extent feasible, from inappropriate access, modification, dissemination, and destruction. As noted above, however, this final rule has been modified to increase flexibility

as to how this protection is accomplished.

p. Comment: One commenter stated that all sections regarding confidentiality and privacy should be removed, since they do not belong in this regulation.

Response: As the discussion in section III.A above of this final rule makes clear, the privacy and security standards are very closely related. Section 1173(d)(2) of the Act specifically mentions "confidentiality" and authorizes uses and disclosures of information as part of what security safeguards must address. Thus, we cannot omit all references to confidentiality and privacy in discussions of the security standards. However, we have relocated material that relates to both security and privacy (including definitions) to the general section of part 164.

q. Comment: One commenter asked that data retention be addressed more specifically, since this will become a significant issue over time. It is recommended that a national work group be convened to address this issue.

Response: The commenter's concern is noted. While the documentation relating to Security Rule implementation must be retained for a period of 6 years (see § 164.316(b)(2)), it is not within the scope of this final

rule to address data retention time frames for administrative or clinical records.

r. Comment: One commenter stated that requiring provider practices to develop policies, procedures, and training programs and to implement record keeping and documentation systems would be tremendously resource-intensive and increase the costs of health care.

Response: We expect that many of the standards of this final rule are already being met in one form or another by covered entities. For example, as part of normal business operations, health care providers already take measures to protect the health information in their keeping. Health care providers already keep records, train their employees, and require employees to follow office policies and procedures. Similarly, health plans are already frequently required by State law to keep information confidential. While revisions to a practice's or plan's current activities may be necessary, the development of entirely new systems or procedures may not be necessary.

s. Comment: One commenter stated that there is no system for which risk has been eliminated and expressed concern over phrases such as covered entities must "assure

that electronic health information pertaining to an individual remains secure."

Response: We agree with the commenter that there is no such thing as a totally secure system that carries no risks to security. Furthermore, we believe the Congress' intent in the use of the word "ensure" in section 1173(d) of the Act was to set an exceptionally high goal for the security of electronic protected health information. However, we note that the Congress also recognized that some trade-offs would be necessary, and that "ensuring" protection did not mean providing protection, no matter how expensive. See section 1173(d)(1)(A)(ii) of the Act. Therefore, when we state that a covered entity must ensure the safety of the information in its keeping, we intend that a covered entity take steps, to the best of its ability, to protect that information. This will involve establishing a balance between the information's identifiable risks and vulnerabilities, and the cost of various protective measures, and will also be dependent upon the size, complexity, and capabilities of the covered entity, as provided in § 164.306(b).

E. Administrative Safeguards (§ 164.308)

We proposed that measures taken to comply with the

rule be appropriate to protect the health information in a covered entity's care. Most importantly, we proposed to require that both the measures taken and documentation of those measures be kept current, that is, reviewed and updated periodically to continue appropriately to protect the health information in the care of covered entities. We would have required the documentation to be made available to those individuals responsible for implementing the procedure.

We proposed a number of administrative requirements and supporting implementation features, and required documentation for those administrative requirements and implementation features.

In this final rule, we have placed these administrative standards in § 164.308. We have reordered them, deleted much of the detail of the proposed requirements, as discussed below, and omitted two of the proposed sets of requirements (system configuration requirements and a requirement for a formal mechanism for processing records) as discussed in paragraph 10 of the discussion of § 164.308 of section III.E. of this preamble. Otherwise, the basic elements of the administrative safeguards are adopted in this final rule as proposed.

1. Security management process (§ 164.308(a)(1)(i)).

We proposed the establishment of a formal security management process to involve the creation, administration, and oversight of policies to address the full range of security issues and to ensure the prevention, detection, containment, and correction of security violations. This process would include implementation features consisting of a risk analysis, risk management, and sanction and security policies.

We also proposed, in a separate requirement under administrative procedures, an internal audit, which would be an in-house review of the records of system activity (for example, logins, file accesses, and security incidents) maintained by an entity.

In this final rule, risk analysis, risk management, and sanction policy are adopted as required implementation specifications although some of the details are changed, and the proposed internal audit requirement has been renamed as "information system activity review" and incorporated here as an additional implementation specification.

a. Comment: Three commenters asked that this requirement be deleted. Two commenters cited this

requirement as a possible burden. Several commenters asked that the implementation features be made optional.

Response: This standard and its component implementation specifications form the foundation upon which an entity's necessary security activities are built. See NIST SP 800-30, "Risk Management Guide for Information Technology Systems," chapters 3 and 4, January 2002. An entity must identify the risks to and vulnerabilities of the information in its care before it can take effective steps to eliminate or minimize those risks and vulnerabilities. Some form of sanction or punishment activity must be instituted for noncompliance. Indeed, we question how the statutory requirement for safeguards "to ensure compliance . . . by a [covered entity's] officers and employees" could be met without a requirement for a sanction policy. See section 1176(d)(2)(C) of the Act. Accordingly, implementation of these specifications remains mandatory. However, it is important to note that covered entities have the flexibility to implement the standard in a manner consistent with numerous factors, including such things as, but not limited to, their size, degree of risk, and environment. We have deleted the implementation specification calling for an organizational security

policy, as it duplicated requirements of the security management and training standard.

We note that the implementation specification for a risk analysis at § 164.308(a)(1)(ii)(A) does not specifically require that a covered entity perform a risk analysis often enough to ensure that its security measures are adequate to provide the level of security required by § 164.306(a). In the proposed rule, an assurance of adequate security was framed as a requirement to keep security measures "current." We continue to believe that security measures must remain current, and have added regulatory language in § 164.306(e) as a more precise way of communicating that security measures in general that must be periodically reassessed and updated as needed.

The risk analysis implementation specification contains other terms that merit explanation. Under § 164.308(a)(1)(ii)(A), the risk analysis must look at risks to the covered entity's electronic protected health information. A thorough and accurate risk analysis would consider "all relevant losses" that would be expected if the security measures were not in place. "Relevant losses" would include losses caused by unauthorized uses and disclosures and loss of data integrity that would be

expected to occur absent the security measures.

b. Comment: Relative to the development of an entity's sanction policy, one commenter asked that we describe the sanction penalties for breach of security. Another suggested establishment of a standard to which one's conduct could be held and adoption of mitigating circumstances so that the fact that a person acted in good faith would be a factor that could be used to reduce or otherwise minimize any sanction imposed. Another commenter suggested sanction activities not be implemented before the full implementation and testing of all electronic transaction standards.

Response: The sanction policy is a required implementation specification because--(1) the statute requires covered entities to have safeguards to ensure compliance by officers and employees; (2) a negative consequence to noncompliance enhances the likelihood of compliance; and (3) sanction policies are recognized as a usual and necessary component of an adequate security program. The type and severity of sanctions imposed, and for what causes, must be determined by each covered entity based upon its security policy and the relative severity of the violation.

c. Comment: Commenters requested the definitions of "risk analysis" and "breach."

Response: "Risk analysis" is defined and described in the specification of the security management process standard, and is discussed in the preamble discussion of § 164.308(a)(1)(ii)(A) of this final rule. The term breach is no longer used and is, therefore, not defined.

d. Comment: One commenter asked whether all health information is considered equally "sensitive," the thought being that, in determining risk, an entity may consider the loss of a smaller amount of extraordinarily sensitive data to be more significant than the loss of a larger amount of routinely collected data. The commenter stated that common reasoning would suggest that the smaller amount of data would be considered more sensitive.

Response: All electronic protected health information must be protected at least to the degree provided by these standards. If an entity desires to protect the information to a greater degree than the risk analysis would indicate, it is free to do so.

e. Comment: One commenter asked that we add "threat assessment" to this requirement.

Response: We have not done this because we view

threat assessment as an inherent part of a risk analysis; adding it would be redundant.

f. Comment: We proposed a requirement for internal audit, the in-house review of the records of system activity (for example, logins, file accesses, and security incidents) maintained by an entity. Several commenters wanted this requirement deleted. One suggested the audit trail requirement should not be mandatory, while another stated that internal audits would be unnecessary if physical security requirements are implemented.

A number of commenters asked that we clarify the nature and scope of what an internal audit covers and what the audit time frame should be. Several commenters offered further detail concerning what should and should not be required in an internal audit for security purposes. One commenter stated that ongoing intrusion detection should be included in this requirement. Another wanted us to specify the retention times for archived audit logs.

Several commenters had difficulty with the term "audit" and suggested we change the title of the requirement to "logging and violation monitoring."

A number of commenters stated this requirement could result in an undue burden and would be economically

unfeasible.

Response: Our intent for this requirement was to promote the periodic review of an entity's internal security controls, for example, logs, access reports, and incident tracking. The extent, frequency, and nature of the reviews would be determined by the covered entity's security environment. The term "internal audit" apparently, based on the comments received, has certain rigid formal connotations we did not intend. We agree that the implementation of formal internal audits could prove burdensome or even unfeasible, to some covered entities due to the cost and effort involved. However, we do not want to overlook the value of internal reviews. Based on our review of the comments and the text to which they refer, it is clear that this requirement should be renamed for clarity and that it should actually be an implementation specification of the security management process rather than an independent standard. We accordingly remove "internal audit" as a separate requirement and add "information system activity review" under the security management process standard as a mandatory implementation specification.

2. Assigned Security Responsibility (§ 164.308(a)(2))

We proposed that the responsibility for security be assigned to a specific individual or organization to provide an organizational focus and importance to security, and that the assignment be documented. Responsibilities would include the management and supervision of (1) the use of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data.

In this final rule, we clarify that the final responsibility for a covered entity's security must be assigned to one official. The requirement for documentation is retained, but is made part of § 164.316 below. This policy is consistent with the analogous policy in the Privacy Rule, at 45 CFR 164.530(a), and the same considerations apply. See 65 FR 82744 through 87445. The same person could fill the role for both security and privacy.

a. Comment: Commenters were concerned that delegation of assigned security responsibility, especially in large organizations, needs to be to more than a single individual. Commenters believe that a large health organization's security concerns would likely cross many departmental boundaries requiring group responsibility.

Response: The assigned security responsibility standard adopted in this final rule specifies that final security responsibility must rest with one individual to ensure accountability within each covered entity. More than one individual may be given specific security responsibilities, especially within a large organization, but a single individual must be designated as having the overall final responsibility for the security of the entity's electronic protected health information. This decision also aligns this rule with the final Privacy Rule provisions concerning the Privacy Official.

b. Comment: One commenter disagreed with placing assigned security responsibility as part of physical safeguards. The commenter suggested that assigned security responsibility should be included under the Administrative Procedures.

Response: Upon review of the matrix and regulations text, we agree with the commenter, because this requirement involves an administrative decision at the highest levels of who should be responsible for ensuring security measures are implemented and maintained. Assigned security responsibility has been removed from "Physical safeguards" and is now located under "Administrative safeguards" at

§ 164.308.

3. Workforce Security (§ 164.308(a)(3)(i))

We proposed implementation of a number of features for personnel security, including ensuring that maintenance personnel are supervised by a knowledgeable person, maintaining a record of access authorizations, ensuring that operating and maintenance personnel have proper access authorization, establishing personnel clearance procedures, establishing and maintaining personnel security policies and procedures, and ensuring that system users have proper training.

In this final rule, to provide clarification and reduce duplication, we have combined the "Assure supervision of maintenance personnel by authorized, knowledgeable person" implementation feature and the "Operating, and in some cases, maintenance personnel have proper access authorization" feature into one addressable implementation specification titled "Authorization and/or supervision."

In a related, but separate, requirement entitled "Termination procedures," we proposed implementation features for the ending of an employee's employment or an internal or external user's access. These features would

include things such as changing combination locks, removal from access lists, removal of user account(s), and the turning in of keys, tokens, or cards that allow access.

In this final rule, "Termination procedures" has been made an addressable implementation specification under "Workforce security." This is addressable because in certain circumstances, for example, a solo physician practice whose staff consists only of the physician's spouse, formal procedures may not be necessary.

The proposed "Personnel security policy/procedure" and "record of access authorizations" implementation features have been removed from this final rule, as they have been determined to be redundant. Implementation of the balance of the "Workforce security" implementation specifications and the other standards contained within this final rule will result in assurance that all personnel with access to electronic protected health information have the required access authority as well as appropriate clearances.

a. Comment: The majority of comments concerned the supervision of maintenance personnel by an authorized knowledgeable person. Commenters stated this would not be feasible in smaller settings. For example, the availability of technically knowledgeable persons to ensure

this supervision would be an issue. We were asked to either reword this implementation feature or delete it.

Response: We agree that a "knowledgeable" person may not be available to supervise maintenance personnel. We have accordingly modified this implementation specification so that, in this final rule, we are adopting an addressable implementation specification titled, "Authorization and/or supervision," requiring that workforce members, for example, operations and maintenance personnel, must either be supervised or have authorization when working with electronic protected health information or in locations where it resides (see § 164.308(a)(3)(ii)(A)). Entities can decide on the feasibility of meeting this specification based on their risk analysis.

b. Comment: The second largest group of comments requested assurance that, with regard to the proposed "Personnel clearance procedure" implementation feature, having appropriate clearances does not mean performing background checks on everyone. We were asked to delete references to "clearance" and use the term "authorization" in its place.

Response: We agree with the commenters concerning background checks. This feature was not intended to be

interpreted as an absolute requirement for background checks. We retain the use of the term "clearance," however, because we believe that it more accurately conveys the screening process intended than does the term "authorization." We have attempted to clarify our intent in the language of § 164.308(a)(3)(ii)(B), which now reads, "Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate." The need for and extent of a screening process is normally based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective personnel screening processes may be applied in a way to allow a range of implementation, from minimal procedures to more stringent procedures based on the risk analysis performed by the covered entity. So long as the standard is met and the underlying standard of § 164.306(a) is met, covered entities have choices in how they meet these standards. To clarify the intent of this provision, we retitle the implementation specification "Workforce clearance procedure."

c. Comment: One commenter asked that we expand the implementation features to include the identification of the restrictions that should be placed on members of the

workforce and others.

Response: We have not adopted this comment in the interest of maintaining flexibility as discussed in § 164.306. Restrictions would be dependent upon job responsibilities, the amount and type of supervision required and other factors. We note that a covered entity should consider in this regard the applicable requirements of the Privacy Rule (see, for example, § 164.514(d)(2) (relating to minimum necessary requirements), and § 164.530(c) (relating to safeguards).

d. Comment: One commenter believes that the proposed "Personnel security" requirement was reasonable, since an administrative determination of trustworthiness is needed before allowing access to sensitive information. Two commenters asked that we delete the requirement entirely. A number of commenters requested that we delete the implementation features. Another commenter stated that all the implementation features may not be applicable or even appropriate to a given entity and should be so qualified.

Response: While we do not believe this requirement should be eliminated, we agree that all the implementation specifications may not be applicable or even appropriate to a given entity. For example, a personal clearance may not

be reasonable or appropriate for a small provider whose only assistant is his or her spouse. The implementation specifications are not mandatory, but must be addressed. This final rule has been changed to reflect this approach (see § 164.308(a)(3)(ii)(B)).

e. Comment: The majority of commenters on the "Termination procedures" requirement asked that it be made optional, stating that it may not be applicable or even appropriate in all circumstances and should be so qualified or posed as guidelines. A number of commenters stated that the requirement should be deleted. One commenter stated that much of the material covered under the "Termination procedures" requirement is already covered in "Information access control." A number of commenters stated that this requirement was too detailed and some of the requirements excessive.

Response: Based upon the comments received, we agree that termination procedures should not be a separate standard; however, consideration of termination procedures remains relevant for any covered entity with employees, because of the risks associated with the potential for unauthorized acts by former employees, such as acts of retribution or use of proprietary information for personal

gain. We further agree with the reasoning of the commenters who asked that these procedures be made optional; therefore, "Termination procedures" is now reflected in this final rule as an addressable implementation specification. We also removed reference to all specific termination activities, for example, changing locks, because, although the activities may be considered appropriate for some covered entities, they may not be reasonable for others.

f. Comment: One commenter asked whether human resource employee termination policies and procedures must be documented to show the types of security breaches that would result in termination.

Response: Policies and procedures implemented to adhere to this standard must be documented (see § 164.316 below). The purpose of termination procedure documentation under this implementation specification is not to detail when or under which circumstances an employee should be terminated. This information would more appropriately be part of the entity's sanction policy. The purpose of termination procedure documentation is to ensure that termination procedures include security-unique actions to be followed, for example, revoking passwords and retrieving

keys when a termination occurs.

4. Information Access Management (§ 164.308(a)(4))

We proposed an "information access control" requirement for establishment and maintenance of formal, documented policies and procedures defining levels of access for all personnel authorized to access health information, and how access is granted and modified. In § 164.308(a)(4)(ii)(B) and (C) below, the proposed implementation features are made addressable specifications. We have added in § 164.308(a)(4)(ii)(A), a required implementation specification to isolate health care clearinghouse functions to address the provisions of section 1173(d)(1)(B) of the Act which related to this area.

a. Comment: One commenter asked that the requirement be deleted, expressing the opinion that this requirement goes beyond "reasonable boundaries" into regulating common business practices. In contrast, another asked that we expand this requirement to identify participating parties and access privileges relative to specific data elements.

Response: We disagree that this requirement improperly imposes upon business functions. Restricting access to those persons and entities with a need for access

is a basic tenet of security. By this mechanism, the risk of inappropriate disclosure, alteration, or destruction of information is minimized. We cannot, however, specifically identify participating parties and access privileges relative to data elements within this regulation. These will vary depending upon the entity, the needs within the user community, the system in which the data resides, and the specific data being accessed. This standard is consistent with § 164.514(d) in the Privacy Rule (minimum necessary requirements for use and disclosure of protected health information), and is, therefore, being retained.

b. Comment: Several commenters asked that we not mandate the implementation features, but leave them as optional, a suggested means of compliance. The commenters noted that this might make the rules more scalable and flexible, since this approach would allow providers to implement safeguards that best addressed their needs. Along this line, one commenter expressed the belief that each organization should implement features deemed necessary based on its own risk assessment.

Response: While the information access management standard in this final rule must be met, we agree that the implementation specifications at § 164.308(a)(4)(ii)(B) and

(C) should not be mandated but posed as a suggested means of compliance, which must be addressed. These specifications may not be applicable to all entities based on their size and degree of automation. A fully automated covered entity spanning multiple locations and involving hundreds of employees may determine it has a need to adopt a formal policy for access authorization, while a small provider may decide that a desktop standard operating procedure will meet the specifications. The final rule has been revised accordingly.

c. Comment: Clarification was requested concerning the meaning of "formal."

Response: The word "formal" has caused considerable concern among commenters, as it was thought "formal" carried the connotation of a rigidly defined structure similar to what might be found in the Department of Defense instructions. As used in the proposed rule, this word was not intended to convey such a strict structure. Rather, it was meant to convey that documentation should be an official organizational statement as opposed to word-of-mouth or cryptic notes scratched on a notepad. While documentation is still required (see § 164.316), to alleviate confusion, the word "formal" has been deleted.

d. Comment: One commenter asked that we clarify that this requirement relates to both the establishment of policies for the access control function and to access control (the implementation of those policies).

Response: "Information access management" does address both the establishment of access control policies and their implementation. We use the term "implement" to clarify that the procedures must be in use, and we believe that the requirement to implement policies and procedures requires, as an antecedent condition, the establishment or adaptation of those policies and procedures.

5. Security Awareness and Training (§ 164.308(a)(5)(i))

We proposed, under the requirement "Training," that security training be required for all staff, including management. Training would include awareness training for all personnel, periodic security reminders, user education concerning virus protection, user education in the importance of monitoring login success/failure, and how to report discrepancies, and user education in password management.

In this final rule, we adopt this proposed requirement in modified form. For the standard "Security awareness and training," in § 164.308(a)(5), we require training of the

workforce as reasonable and appropriate to carry out their functions in the facility. All proposed training features have been combined as implementation specifications under this standard. Specific implementation specifications relative to content are addressable. The "Virus protection" implementation feature has been renamed "protection from malicious software," because we did not intend by the nomenclature to exclude coverage of malicious acts that might not come within the prior term, such as worms.

a. Comment: One commenter believes that security awareness training for all system users would be too difficult to do in a large organization.

Response: We disagree with the commenter. Security awareness training is a critical activity, regardless of an organization's size. This feature would typically become part of an entity's overall training program (which would include privacy and other information technology items as well). For example, the Government Information Systems Reform ACT (GISRA) of 2000 requires security awareness training as part of Federal agencies' information security programs, including Federal covered entities, such as the Medicare program. In addition, National Institute of

Standards and Technology (NIST) SP 800-16, Information Technology Security Training Requirements, A role and performance base model, April 1998, provides an excellent source of information and guidance on this subject and is targeted at industry as well as government activities. We also note that covered entities must have discretion in how they implement the requirement, so they can incorporate this training in other existing activities. One approach would be to require this training as part of employee orientation.

b. Comment: A number of commenters asked that this requirement be made optional or used as a guideline only. Several commenters stated that this requirement is too specific and is burdensome. Several asked that the implementation features be removed.

Several others stated that this requirement is not appropriate for agents or contractors. One commenter asked how to apply this requirement to outsiders having access to data. Another asked if this requirement included all subcontractor staff. Others stated that contracts, signed by entities such as consultants, that address training should be sufficient.

Response: Security training remains a requirement because of its criticality; however, we have revised the implementation specifications to indicate that the amount and type of training needed will be dependent upon an entity's configuration and security risks. Business associates must be made aware of security policies and procedures, whether through contract language or other means. Covered entities are not required to provide training to business associates or anyone else that is not a member of their workforce.

c. Comment: Several commenters questioned why security awareness training appeared in two places, under "Physical safeguards" as well as "Administrative safeguards." Others questioned the appropriateness of security awareness training under "Physical safeguards."

Response: We reviewed the definitions of the proposed "Awareness training for all personnel" ("Administrative safeguards") implementation feature and the proposed "Security awareness training" ("Physical safeguards") requirement. We agree that, to avoid confusion and eliminate redundancy, security awareness and training should appear in only one place. We believe the appropriate location for it is under "Administrative

safeguards," as such training is essentially an administrative function.

d. Comment: Several commenters objected to the blanket requirement for security awareness training of individuals who may be on site for a limited time period (for example, a single day).

Response: Each individual who has access to electronic protected health information must be aware of the appropriate security measures to reduce the risk of improper access, uses, and disclosures. This requirement does not mean lengthy training is appropriate in every instance; there are alternative methods to inform individuals of security responsibilities (for example, provisions of pamphlets or copies of security policies, and procedures).

e. Comment: One commenter asked that "training" be changed to "orientation."

Response: We believe the term "training," as presented within this rule is the more appropriate term. The rule does not contemplate a one-time type of activity as connoted by "orientation," but rather an on-going, evolving process as an entity's security needs and procedures change.

f. Comment: Several commenters asked how often training should be conducted and asked for a definition of "periodic," as it appears in the proposed implementation feature "Periodic security reminders." One asked if the training should be tailored to job need.

Response: Amount and timing of training should be determined by each covered entity; training should be an on-going, evolving process in response to environmental and operational changes affecting the security of electronic protected health information. While initial training must be carried out by the compliance date, we provide flexibility for covered entities to construct training programs. Training can be tailored to job need if the covered entity so desires.

6. Security Incident Procedures (§ 164.308(a)(6))

We proposed a requirement for implementation of accurate and current security incident procedures: formal, documented report and response procedures so that security violations would be reported and handled promptly. We adopt this standard in the final rule, along with an implementation specification for response and reporting, since documenting and reporting incidents, as well as responding to incidents are an integral part of a security

program.

a. Comment: Several commenters asked that we further define the scope of a breach of security. Along this same line, another commenter stated that the proposed security incident procedures were too vague as stated. We were asked to specify what a security incident would be, what the internal chain for reporting procedures would be, and what should be included in the documentation (for example, hardware/software, personnel responses).

Response: We define a security incident in § 164.304. Whether a specific action would be considered a security incident, the specific process of documenting incidents, what information should be contained in the documentation, and what the appropriate response should be will be dependent upon an entity's environment and the information involved. An entity should be able to rely upon the information gathered in complying with the other security standards, for example, its risk assessment and risk management procedures and the privacy standards, to determine what constitutes a security incident in the context of its business operations.

b. Comment: One commenter asked what types of incidents must be reported to outside entities. Another

commented that we clarify that incident reporting is internal.

Response: Internal reporting is an inherent part of security incident procedures. This regulation does not specifically require any incident reporting to outside entities. External incident reporting is dependent upon business and legal considerations.

c. Comment: One commenter stated that network activity should be included here.

Response: We see no reason to exclude network activity under this requirement. Improper network activity should be treated as a security incident, because, by definition, it represents an improper instance of access to or use of information.

d. Comment: One commenter stated that this requirement should address suspected misuse also.

Response: We agree that security incidents include misuse of data; therefore, this requirement is addressed.

e. Comment: Several commenters asked that this requirement be deleted. One commenter asked that we delete the implementation features.

Response: As indicated above, we have adopted the proposed standard and combined the implementation

specifications.

7. Contingency Plan (§ 164.308(a)(7)(i))

We proposed that a contingency plan must be in effect for responding to system emergencies. The plan would include an applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures.

In this final rule, we make the implementation specifications for testing and revision procedures and an applications and data criticality analysis addressable, but otherwise require that the contingency features proposed be met.

a. Comment: Several commenters suggested the contingency plan requirement be deleted. Several thought that this aspect of the proposed regulation went beyond its intended scope. Another believed that more discussion and development is needed before developing regulatory guidance on contingency plans. Others wanted this to be an optional requirement. In contrast, one commenter requested more guidance concerning contingency planning. Still others wanted to require that a contingency plan be in place but stated that we should not regulate its contents. One comment stated that data backup, disaster recovery, and

emergency mode operation should not be part of this requirement.

Response: A contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed.

Each entity needs to determine its own risk in the event of an emergency that would result in a loss of operations. A contingency plan may involve highly complex processes in one processing site, or simple manual processes in another. The contents of any given contingency plan will depend upon the nature and configuration of the entity devising it.

While the contingency plan standard must be met, we agree that the proposed testing and revision implementation feature should be an addressable implementation specification in this final rule. Dependent upon the size, configuration, and environment of a given covered entity, the entity should decide if testing and revision of all parts of a contingency plan should be done or if there are more reasonable alternatives. The same is true for the proposed applications and data criticality analysis

implementation feature. We have revised the final rule to reflect this approach.

b. Comment: One commenter believed that adhering to this requirement could prove burdensome. Another stated that testing of certain parts of a contingency plan would be burdensome, and even infeasible, for smaller entities.

Response: Without contingency planning, a covered entity has no assurance that its critical data could survive an emergency situation. Recent events, such as September 11, 2001, illustrate the importance of such planning. Contingency planning will be scalable based upon, among other factors, office configuration, and risk assessment. However, in response to the scalability issue raised by the commenter, we have made the testing and revision implementation specification addressable (see § 164.308(a)(7)(ii)).

c. Comment: Two commenters considered a 2-year implementation time frame for this requirement inadequate for large health plans. Another commenter stated that implementation of measures against natural disaster would be too big an issue for this regulation.

Response: The statute sets forth the compliance dates for the initial standards. The statute requires that

compliance with initial standards is not later than 2 years after adoption of the standards for all covered entities except small health plans for which the compliance date is not later than 3 years after adoption.

The final rule calls for covered entities to consider how natural disasters could damage systems that contain electronic protected health information and develop policies and procedures for responding to such situations. We consider this to be a reasonable precautionary step to take since in many cases the risk would be deemed to be low.

d. Comment: A commenter requested clarification of the term "Emergency mode" with regard to the proposed "Emergency mode operation plan" implementation feature.

Response: We have clarified the "Emergency mode operations plan" to show that it only involves those critical business processes that must occur to protect the security of electronic protected health information during and immediately after a crisis situation.

8. Evaluation (§ 164.308(a)(8))

We proposed that certification would be required and could be performed internally or by an external accrediting agency. We solicited input on appropriate mechanisms to permit an independent assessment of compliance. We were particularly interested in input from those engaging in health care electronic data interchange (EDI), as well as independent certification and auditing organizations addressing issues of documentary evidence of steps taken for compliance; need for, or desirability of, independent verification, validation, and testing of system changes; and certifications required for off-the-shelf products used to meet the requirements of this regulation. We also solicited comments on the extent to which obtaining external certification would create an undue burden on small or rural providers.

In this final rule, we require covered entities to periodically conduct an evaluation of their security safeguards to demonstrate and document their compliance with the entity's security policy and the requirements of this subpart. Covered entities must assess the need for a new evaluation based on changes to their security environment since their last evaluation, for example, new

technology adopted or responses to newly recognized risks to the security of their information.

a. Comment: We received several comments that certification should be performed externally. A larger group of commenters preferred self-certification. The majority of the comments, however, were to the effect that external certification should be encouraged but not mandated.

A number of commenters thought that mandating external certification would create an undue financial burden, regardless of the size of the entity being certified. One commenter stated that external certification would not place an undue burden on a small or rural provider.

Response: Evaluation by an external entity is a business decision to be left to each covered entity. Evaluation is required under § 164.308(a)(8), but a covered entity may comply with this standard either by using its own workforce or an external accreditation agency, which would be acting as a business associate. External evaluation may be too costly an option for small entities.

b. Comment: Several commenters stated that the certification should cover all components of the proposed rule, not just the information systems.

Response: We agree. We have revised this section to reflect that evaluation would be both technical and nontechnical components of security.

c. Comment: A number of commenters expressed a desire for the creation of certification guides or models to complement the rule.

Response: We agree that creation of compliance guidelines or models for different business environments would help in the implementation and evaluation of HIPAA security requirements and we encourage professional associations and others to do so. We may develop technical assistance materials, but do not intend to create certification criteria because we do not have the resources to address the large number of different business environments.

d. Comment: Some commenters asked how certification is possible without specifying the level of risk that is permissible.

Response: The level of risk that is permissible is specified by § 164.306(a). How such risk is managed will be determined by a covered entity through its security risk analysis and the risk mitigation activities it implements in order to ensure that the level of security required by

§ 164.306 is provided.

e. Comment: Several commenters requested creation of a list of Federally "certified" security software and off-the-shelf products. Several others stated that this request was not feasible. Regarding certification of off-the-shelf products, one commenter thought this should be encouraged, but not mandated; several thought this would be an impractical endeavor.

Response: While we will not assume the task of certifying software and off-the-shelf products for the reason described above, we have noted with interest that other Government agencies such as the National Institute of Standards and Technology (NIST) are working towards that end. The health care industry is encouraged to monitor the activity of NIST and provide comments and suggestions when requested (see http://www.niap.nist.gov.).

f. Comment: One commenter stated, "With HCFA's publishing of these HIPAA standards, and their desire to retain the final responsibility for determining violations and imposing penalties of the statute, it also seems appropriate for HCFA to also provide certifying services to ensure security compliance."

Response: In view of the enormous number and variety of covered entities, we believe that evaluation can best be handled through the marketplace, which can develop more usable and targeted evaluation instruments and processes.

8. Business Associate Contracts or Other Arrangements (§ 164.308(b)(1))

In the proposed rule § 142.308(a)(2) "Chain of trust" requirement, we proposed that covered entities be required to enter into a chain of trust partner agreement with their business partners, in which the partners would agree to electronically exchange data and protect the integrity, confidentiality, and availability of the data exchanged. This standard has been modified from the proposed requirement to reflect, in § 164.308(b)(1) "Business associate contracts and other arrangements," the business associate structure put in place by the Privacy Rule.

In this final rule, covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in § 160.103. The covered entity must obtain satisfactory assurances from the business associate that it will appropriately safeguard the information in accordance with these standards (see § 164.314(a)(1)).

The comments received on the proposed chain of trust partner agreements are discussed in section 2 "Business associate contracts and other arrangements" of the discussion of § 164.314 below.

9. Proposed Requirements Not Adopted in This Final Rule

a. Security Configuration Management

We proposed that an organization would be required to implement measures, practices, and procedures regarding security configuration management. They would be coordinated and integrated with other system configuration management practices for the security of information systems. These would include documentation, hardware and/or software installation and maintenance review and testing for security features, inventory procedures, security testing, and virus checking.

Comment: Several commenters asked that the entire requirement be deleted. Several others asked that the inventory and virus checking implementation features be removed as they believe those features are not germane to security configuration management. A number of commenters requested that security testing be deleted because this implementation feature is too detailed, unreasonable, impractical, and beyond the scope of the legislation.

Others stated that the testing would be very complex and expensive. Others wanted more clarification of what we intend by security testing, and how much would be enough. A number of commenters asked that all of the implementation features be deleted. Others asked that the implementation features be made optional. Several commenters wanted to know the scope of organizational integration required. Several others asked if what we meant by Security Configuration Management was change or version control.

Response: Upon review, this requirement appears unnecessary because it is redundant of other requirements we are adopting in this rule. A covered entity will have addressed the activities described by the features under this proposed requirement by virtue of having implemented the risk analysis, risk management measures, sanction policies, and information systems criticality review called for under the security management process. The proposed documentation implementation feature has been made a separate standard (see § 164.316). As a result, the Security Configuration Management requirement is not adopted in this final rule.

b. Formal Mechanism for Processing Records

The proposed rule proposed requiring a formal

mechanism for processing records, and documented policies and procedures for the routine and nonroutine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information. This requirement has not been adopted in the final rule.

Comment: Several commenters thought this requirement concerned the regulation of formal procedures for how an entity does business and stated that such procedures should not be regulated. Others asked for additional clarification of what is meant by this requirement. One commenter thought the requirement too ambiguous and asked for clarification as to whether we meant such things as "the proper handling of storage media, databases, transmissions," or "the clinical realm of processes."

Two commenters asked how extensive this requirement would be and whether systems' user manuals and policies and procedures for handling health information would suffice and what level of detail would be expected.

Several thought this requirement could result in a significant resource and monetary burden to develop and maintain formal procedures. Two asked for an explanation of the benefit to be derived from this requirement.

One asked that covered entities be required to document processes that create a security risk only and suggested that a risk assessment would determine the need for this documentation.

Response: We agree with the commenters that the standard is ambiguous, and upon review, is unnecessary because the remaining standards, for example, device and media controls, provide adequate safeguards. Accordingly, this requirement is not adopted in this final rule.

F. Physical Safeguards (§ 164.310)

We proposed requirements and implementation features for documented physical safeguards to guard data integrity, confidentiality, and availability. We proposed to require safeguards in the following areas: assigned security responsibility; media controls; physical access controls; policies and guidelines on workstation use; a secure workstation location; and security awareness training. A number of specific implementation features were proposed under the media controls and physical access controls requirements.

In § 164.310 of this final rule, most of the proposed implementation features are adopted as addressable implementation specifications. The proposed requirements

for the assigned security responsibility and security awareness training requirements are relocated in § 164.308.

1. General Comments

a. Comment: Several commenters made suggestions to modify the language to more clearly describe "Physical safeguards."

Response: In response to comments, we have revised the definition of "Physical safeguards" to read as follows: "Physical safeguards are security measures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

b. Comment: One commenter was concerned that electronic security systems could not be used in lieu of physical security systems.

Response: This final rule does not preclude the use of electronic security systems in lieu of, or in combination with, physical security systems to meet a "Physical safeguard" standard.

2. Facility Access Controls (§ 164.310(a)(1))

We proposed, under the "Physical access controls" requirement, formal, documented policies and procedures for

limiting physical access to an entity while ensuring that properly authorized access is allowed. These controls would include the following implementation features: disaster recovery, emergency mode operation, equipment control (into and out of site), a facility security plan, procedures for verifying access authorizations before physical access, maintenance records, need-to-know procedures for personnel access, sign-in for visitors and escort, if appropriate, and testing and revision.

In § 164.310(a)(2) below, we combine and restate these as addressable implementation specifications. These are contingency operations, facility security plan, access control and validation procedures, and maintenance records.

a. Comment: Many commenters were concerned because the proposed language would require implementation of all physical access control features. Other commenters were concerned that the language did not allow entities to use the results of their risk assessment and risk management process to arrive at the appropriate solutions for them.

Response: We agree that implementation of all implementation specifications may not be appropriate in all situations. While the facility access controls standard must be met, we agree that the implementation

specifications should not be required in all circumstances, but should be addressable. In this final rule, all four implementation specifications are addressable.

We have also determined, based on "level of detail" comments requesting consolidation of the list of implementation features, that the proposed implementation feature "Equipment control (into and out of site)" was redundant. "Equipment control" is already covered under the "Device and media controls" standard at § 164.310(d)(1). Accordingly, we have eliminated it as a separate implementation specification.

b. Comment: One commenter raised the issue of a potential conflict of authority between those having access to the data and those responsible for checking and maintaining access controls.

Response: Any potential conflicts should be identified, addressed, and resolved in the policies and procedures developed according to the standards under § 164.308.

c. Comment: Several commenters questioned whether "Physical Access Controls" was a descriptive phrase to describe a technology to be used, or whether the phrase referred to a facility.

Response: We agree that the term "Physical" may be misleading; to remove any confusion, the requirement is reflected in this final rule as a standard titled "Facility access controls." We believe this is a more precise term to describe that the standard, and its associated implementation specifications, is applicable to an entity's business location or locations.

d. Comment: Several commenters requested that the disaster recovery and emergency mode operations features be moved to "Administrative safeguards." Other commenters recommended that disaster recovery and emergency mode operations should be replaced by, and included in, a "Contingency Operations" implementation feature.

Response: The "Administrative safeguards" section addresses the contingency planning that must be done to contend with emergency situations. The placement of the disaster recovery and emergency mode operations implementation specifications in the "Physical safeguards" section is also appropriate, however, because "Physical safeguards" defines the physical operations (processes) that provide access to the facility to implement the associated plans, developed under § 164.308. We agree, however, that the term "contingency operations" better

describes, and would include, disaster recovery and emergency mode operations, and have modified the regulation text accordingly (see § 164.310(a)(1)).

e. Comment: Commenters were concerned about having to address in their facility security plan the exterior/interior security of a building when they are one of many occupants rather than the sole occupant. Additional commenters were concerned that the responsibility for physical security of the building could not be delegated to a third party when the covered entity shares the building with other offices.

Response: The facility security plan is an addressable implementation specification. However, the covered entity retains responsibility for considering facility security even where it shares space within a building with other organizations. Facility security measures taken by a third party must be considered and documented in the covered entity's facility security plan, when appropriate.

3. Workstation Use (§ 164.310(b))

We proposed policy and guidelines on workstation use that included documented instructions/procedures delineating the proper functions to be performed and the

manner in which those functions are to be performed (for example, logging off before leaving a workstation unattended) to maximize the security of health information. In this final rule, we adopt this standard.

Comment: One commenter was concerned most people may be misled by the use of "terminal" as an example in the definition of workstation. The concern was that the standard only addresses "fixed location devices," while in many instances the workstation has become a laptop computer.

Response: For clarity, we have added the definition of "workstation" to § 164.304 and deleted the word "terminal" from the description of workstation use in § 164.310(b).

4. Workstation Security (§ 164.310(c))

We proposed that each organization would be required to put in place physical safeguards to restrict access to information. In this final rule, we retain the general requirement for a secure workstation.

Comment: Comments were directed toward the example profiled in the definition of a secure workstation location. It was believed that what constitutes a secure workstation location must be dependent upon the entity's

risk management process.

Response: We agree that what constitutes an appropriate solution to a covered entity's workstation security issues is dependent on the entity's risk analysis and risk management process. Because many commenters incorrectly interpreted the examples as the required and only solution for securing the workstation location, we have modified the regulations text description to generalize the requirement (see § 164.310(c)). Also, for clarity, the title "Secure workstation location" has been changed to "Workstation security" (see also the definition of "Workstation" at § 164.304).

5. Device and Media Controls (§ 164.310(d)(1))

We proposed that covered entities have media controls in the form of formal, documented policies and procedures that govern the receipt and removal of hardware and/or software (for example, diskettes and tapes) into and out of a facility. Implementation features would have included "Access control," "Accountability" (tracking mechanism), "Data backup," "Data storage," and "Disposal."

In this final rule, we adopt most of these provisions as addressable implementation specifications and add a specification for media re-use. We change the name from

"Media controls" to "Device and media controls" to more clearly reflect that this standard concerns hardware as well as electronic media. The proposed "Access control" implementation feature has been removed, as it is addressed as part of other standards (see section III.C.12.c of this preamble).

a. Comment: One commenter was concerned about the exclusion of removable media devices from examples of physical types of hardware and/or software.

Response: The media examples used were not intended to represent all possible physical types of hardware and/or software. Removable media devices, although not specifically listed, are not intended to be excluded.

b. Comment: Comments were made that the issue of equipment re-use or recycling of media containing mass storage was not addressed in "Media controls."

Response: We agree that equipment re-use or recycling should be addressed, since this equipment may contain electronic protected health information. The "Device and media controls" standard is accordingly expanded to include a required implementation specification that addresses the re-use of media (see § 164.310(d)(2)(ii)).

c. Comment: Several commenters asked for a definition of the term "facility," as used in the proposed "Media controls" requirement description. Commenters were unclear whether we were talking about a corporate entity or the physical plant.

Response: The term "facility" refers to the physical premises and the interior and exterior of a building(s). We have added this definition to § 164.304.

d. Comment: Several commenters believe the "Media controls" implementation features are too onerous and should be deleted.

Response: While the "Device and media controls" standard must be met, we believe, based upon further review, that implementation of all specifications would not be necessary in every situation, and might even be counter-productive in some situations. For example, small providers would be unlikely to be involved in large-scale moves of equipment that would require systematic tracking, unlike, for example, large health care providers or health plans. We have, therefore, reclassified the "Accountability and data backup" implementation specification as addressable to provide more flexibility in meeting the standard.

e. Comment: One commenter was concerned about the accountability impact of audit trails on system resources and the pace of system services.

Response: The proposed audit trail implementation feature appears as the addressable "Accountability" implementation specification. The name change better reflects the purpose and intended scope of the implementation specification. This implementation specification does not address audit trails within systems and/or software. Rather it requires a record of the actions of a person relative to the receipt and removal of hardware and/or software into and out of a facility that are traceable to that person. The impact of maintaining accountability on system resources and services will depend upon the complexity of the mechanism to establish accountability. For example, the appropriate mechanism for a given entity may be manual, such as receipt and removal restricted to specific persons, with logs kept. Maintaining accountability in such a fashion should have a minimal, if any, effect on system resources and services.

f. Comment: A commenter was concerned about the resource expenditure (system and fiscal) for total e-mail backup and wanted a clarification of the extensiveness of

data backup.

Response: The data an entity needs to backup, and which operations should be used to carry out the backup, should be determined by the entity's risk analysis and risk management process. The data backup plan, which is part of the required contingency plan (see § 164.308(a)(7)(ii)(A)), should define exactly what information is needed to be retrievable to allow the entity to continue business "as usual" in the face of damage or destruction of data, hardware, or software. The extent to which e-mail backup would be needed would be determined through that analysis.

G. Technical Safeguards (§ 164.312)

We proposed five technical security services requirements with supporting implementation features: Access control; Audit controls; Authorization control; Data authentication; and Entity authentication. We also proposed specific technical security mechanisms for data transmitted over a communications network, Communications/network controls with supporting implementation features; Integrity controls; Message authentication; Access controls; Encryption; Alarm; Audit trails; Entity authentication; and Event reporting.

In this final rule, we consolidate these provisions

into § 164.312. That section now includes standards regarding access controls, audit controls, integrity (previously titled data authentication), person or entity authentication, and transmission security. As discussed below, while certain implementation specifications are required, many of the proposed security implementation features are now addressable implementation specifications. The function of authorization control has been incorporated into the information access management standard under § 164.308, Administrative safeguards.

1. Access Control (§ 164.312(a)(1))

In the proposed rule, we proposed to require that the access controls requirement include features for emergency access procedures and provisions for context-based, role-based, and/or user-based access; we also proposed the optional use of encryption as a means of providing access control. In this final rule, we require unique user identification and provision for emergency access procedures, and retain encryption as an addressable implementation specification. We also make "Automatic logoff" an addressable implementation specification. "Automatic logoff" and "Unique user identification" were formerly implementation features under the proposed "Entity

authentication" (see § 164.312(d)).

a. Comment: Some commenters believe that in specifying "Context," "Role," and "User" based controls, use of other controls would effectively be excluded, for example, "Partition rule-based access controls," and the development of new access control technology.

Response: We agree with the commenters that other types of access controls should be allowed. There was no intent to limit the implementation features to the named technologies and this final rule has been reworded to make it clear that use of any appropriate access control mechanism is allowed. Proposed implementation features titled "Context-based access," "Role-based access," and "User-based access" have been deleted and the access control standard at § 164.312(a)(1) states the general requirement.

b. Comment: A large number of comments were received objecting to the identification of "Automatic logoff" as a mandatory implementation feature. Generally the comments asked that we not be so specific and allow other forms of inactivity lockout, and that this type of feature be made optional, based more on the particular configuration in use and a risk assessment/analysis.

Response: We agree with the comments that mandating an automatic logoff is too specific. This final rule has been written to clarify that the proposed implementation feature of automatic logoff now appears as an addressable access control implementation specification and also permits the use of an equivalent measure.

c. Comment: We received comments asking that encryption be deleted as an implementation feature and stating that encryption is not required for "data at rest."

Response: The use of file encryption is an acceptable method of denying access to information in that file. Encryption provides confidentiality, which is a form of control. The use of encryption, for the purpose of access control of data at rest, should be based upon an entity's risk analysis. Therefore, encryption has been adopted as an addressable implementation specification in this final rule.

d. Comment: We received one comment stating that the proposed implementation feature "Procedure for emergency access," is not access control and recommending that emergency access be made a separate requirement.

Response: We believe that emergency access is a necessary part of access controls and, therefore, is

properly a required implementation specification of the "Access controls" standard. Access controls will still be necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. For example, in a situation when normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or man-made disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed electronic protected health information.

2. Audit Controls (§ 164.312(b))

We proposed that audit control mechanisms be put in place to record and examine system activity. We adopt this requirement in this final rule.

a. Comment: We received a comment stating that "Audit controls" should be an implementation feature rather than the standard, and suggesting that we change the title of the standard to "Accountability," and provide additional detail to the audit control implementation feature.

Response: We do not adopt the term "Accountability" in this final rule because it is not descriptive of the requirement, which is to have the capability to record and

examine system activity. We believe that it is appropriate to specify audit controls as a type of technical safeguard. Entities have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses. For example, see NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems and NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security.

b. Comment: One commenter recommended that this final rule state that audit control mechanisms should be implemented based on the findings of an entity's risk assessment and risk analysis. The commenter asserted that audit control mechanisms should be utilized only when appropriate and necessary and should not adversely affect system performance.

Response: We support the use of a risk assessment and risk analysis to determine how intensive any audit control function should be. We believe that the audit control requirement should remain mandatory, however, since it provides a means to assess activities regarding the electronic protected health information in an entity's care.

c. Comment: One commenter was concerned about the interplay of State and Federal requirements for auditing of privacy data and requested additional guidance on the interplay of privacy rights, laws, and the expectation for audits under the rule.

Response: In general, the security standards will supercede any contrary provision of State law. Security standards in this final rule establish a minimum level of security that covered entities must meet. We note that covered entities may be required by other Federal law to adhere to additional, or more stringent security measures. Section 1178(a)(2) of the statute provides several exceptions to this general rule. With regard to protected health information, the preemption of State laws and the relationship of the Privacy Rule to other Federal laws is discussed in the Privacy Rule beginning at 65 FR 82480; the preemption provisions of the rule are set out at 45 CFR part 160, subpart B.

It should be noted that although the Privacy Rule does not incorporate a requirement for an "audit trail" function, it does call for providing an accounting of certain disclosures of protected health information to an individual upon request. There has been a tendency to

assume that this Privacy Rule requirement would be satisfied via some sort of process involving audit trails. We caution against assuming that the Security Rule's requirement for an audit capability will satisfy the Privacy Rule's requirement regarding accounting for disclosures of protected health information. The two rules cover overlapping, but not identical information. Further, audit trails are typically used to record uses within an electronic information system, while the Privacy Rule requirement for accounting applies to certain disclosures outside of the covered entity (for example, to public health authorities).

3. Integrity (§ 164.312(c)(1))

We proposed under the "Data authentication" requirement, that each organization be required to corroborate that data in its possession have not been altered or destroyed in an unauthorized manner and provided examples of mechanisms that could be used to accomplish this task. We adopt the proposed requirement for data authentication in the final rule as an addressable implementation specification "Mechanism to authenticate data," under the "Integrity" standard.

a. Comment: We received a large number of comments requesting clarification of the "Data authentication" requirement. Many of these comments suggested that the requirement be called "Data integrity" instead of "Data authentication." Others asked for guidance regarding just what "data" must be authenticated. A significant number of commenters indicated that this requirement would put an extraordinary burden on large segments of the health care industry, particularly when legacy systems are in use. Requests were received to make this an "optional" requirement, based on an entity's risk assessment and analysis.

Response: We adopt the suggested "integrity" terminology because it more clearly describes the intent of the standard. We retain the meaning of the term "Data authentication" under the addressable implementation specification "Mechanism to authenticate data," and provide an example of a potential means to achieve data integrity.

Error-correcting memory and magnetic disc storage are examples of the built-in data authentication mechanisms that are ubiquitous in hardware and operating systems today. The risk analysis process will address what data must be authenticated and should provide answers

appropriate to the different situations faced by the various health care entities implementing this regulation.

Further, we believe that this standard will not prove difficult to implement, since there are numerous techniques available, such as processes that employ digital signature or check sum technology to accomplish the task.

b. Comment: We received numerous comments suggesting that "Double keying" be deleted as a viable "Data authentication" mechanism, since this practice was generally associated with the use of punched cards.

Response: We agree that the process of "Double keying" is outdated. This final rule omits any reference to "Double keying."

4. Person or Entity Authentication (§ 164.312(d))

We proposed that an organization implement the requirement for "Entity authentication", the corroboration that an entity is who it claims to be. "Automatic logoff" and "Unique user identification" were specified as mandatory features, and were to be coupled with at least one of the following features: (1) a "biometric" identification system; (2) a "password" system; (3) a "personal identification number"; and (4) "telephone callback," or a "token" system that uses a physical device

for user identification.

In this final rule, we provide a general requirement for person or entity authentication without the specifics of the proposed rule.

Comment: We received comments from a number of organizations requesting that the implementation features for entity authentication be either deleted in their entirety or at least be made optional. On the other hand, comments were received requesting that the use of digital signatures and soft tokens be added to the list of implementation features.

Response: We agree with the commenters that many different mechanisms may be used to authenticate entities, and this final rule now reflects this fact by not incorporating a list of implementation specifications, in order to allow covered entities to use whatever is reasonable and appropriate. "Digital signatures" and "soft tokens" may be used, as well as many other mechanisms, to implement this standard.

The proposed mandatory implementation feature, "Unique user identification," has been moved from this standard and is now a required implementation specification under "Access control" at § 164.312(a)(1). "Automatic logoff"

has also been moved from this standard to the "Access control" standard and is now an addressable implementation specification.

5. Transmission Security (§ 164.312(e)(1))

Under "Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted Over a Communications Network," we proposed that "Communications/network controls" be required to protect the security of health information when being transmitted electronically from one point to another over open networks, along with a combination of mandatory and optional implementation features. We proposed that some form of encryption must be employed on "open" networks such as the internet or dial-up lines.

In this final rule, we adopt integrity controls and encryption, as addressable implementation specifications.

a. Comment: We received a number of comments asking for overall clarification as well as a definition of terms used in this section. A definition for the term "open networks" was the most requested action, but there was a general expression of dislike for the manner in which we approached this section, with some comments suggesting that the entire section be rewritten. A significant number of

comments were received on the question of encryption requirements when dial-up lines were to be employed as a means of connectivity. The overwhelming majority strongly urged that encryption not be mandatory when using any transmission media other than the Internet, but rather be considered optional based on individual entity risk assessment/analysis. Many comments noted that there are very few known breaches of security over dial-up lines and that nonjudicious use of encryption can adversely affect processing times and become both financially and technically burdensome. Only one commenter suggested that "most" external traffic should be encrypted.

Response: In general, we agree with the commenters who asked for clarification and revision. This final rule has been significantly revised to reflect a much simpler and more direct requirement. The term "Communications/network controls" has been replaced with "Transmission security" to better reflect the requirement that, when electronic protected health information is transmitted from one point to another, it must be protected in a manner commensurate with the associated risk.

We agree with the commenters that switched, point-to-point connections, for example, dial-up lines, have a very

small probability of interception.

Thus, we agree that encryption should not be a mandatory requirement for transmission over dial-up lines. We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. Particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting e-mail communications with patients. As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification. Covered entities are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the internet.

As business practices and technology change, there may arise situations where electronic protected health information being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis showed such risk to be significant, we would expect covered entities to encrypt those transmissions, if appropriate, under the addressable implementation specification for encryption.

We do not use the term "open network" in this final rule because its meaning is too broad. We include as an addressable implementation specification the requirement that transmissions be encrypted when appropriate based on the entity's risk analysis.

b. Comment: We received comments requesting that the implementation features be deleted or made optional. Three commenters asked that the requirement for an alarm be deleted.

Response: This final rule has been revised to reflect deletion of the following implementation features: (1) the alarm capability; (2) audit trail; (3) entity authentication; and (4) event reporting. These features were associated with a proposed requirement for "Communications/network controls" and have been deleted since they are normally incorporated by telecommunications providers as part of network management and control functions that are included with the provision of network services. A health care entity would not expect to be responsible for these technical telecommunications features. "Access controls" has also been deleted from the implementation features since the consideration of the use of encryption will satisfy the intent of this feature. We

retain as addressable implementation specifications two features: (1) "integrity controls" and "encryption". "Message authentication" has been deleted as an implementation feature because the use of data authentication codes (called for in the "integrity controls" implementation specification) satisfies the intent of "Message authentication."

c. Comment: A number of comments were received asking that this final rule establish a specific (or at least a minimum) cryptographic algorithm strength. Others recommended that the rule not specify an encryption strength since technology is changing so rapidly. Several commenters requested guidelines and minimum encryption standards for the Internet. Another stated that, since an example was included (small or rural providers for example), the government should feel free to name a specific encryption package. One commenter stated that the requirement for encryption on the Internet should reference the "CMS Internet Security Policy."

Response: We remain committed to the principle of technology neutrality and agree with the comment that rapidly changing technology makes it impractical and inappropriate to name a specific technology. Consistent

with this principle, specification of an algorithm strength or specific products would be inappropriate. Moreover, rapid advances in the success of "brute force" cryptanalysis techniques suggest that any minimum specification would soon be outmoded. We maintain that it is much more appropriate for this final rule to state a general requirement for encryption protection when necessary and depend on covered entities to specify technical details, such as algorithm types and strength. Because "CMS Internet Security Policy" is the policy of a single organization and applies only to information sent to CMS, and not between all covered entities, we have not referred to it here.

d. Comment: The proposed definition of "Integrity controls" generated comments that asked that the word "validity" be changed to "Integrity." Commenters were concerned about the ability of an entity to ensure that information was "valid."

Response: We agree with the commenters about the meaning of the word "validity" in the context of the proposed definition of "Integrity controls." We have named "integrity controls" as an implementation specification in this final rule to require mechanisms to ensure that

electronically transmitted information is not improperly modified without detection (see § 164.312(c)(1)).

e. Comment: Three commenters asked for clarification and guidance regarding the unsolicited electronic receipt of health information in an unsecured manner, for example, when the information was submitted by a patient via e-mail over the Internet. Commenters asked for guidance as to what was their obligation to protect data received in this manner.

Response: The manner in which electronic protected health information is received by a covered entity does not affect the requirement that security protection must subsequently be afforded to that information by the covered entity once that information is in possession of the covered entity.

6. Proposed Requirements Not Adopted in This Final Rule

a. Authorization Control

We proposed, under "Technical Security Services to Guard Data Integrity, Confidentiality, and Availability," that a mechanism be required for obtaining consent for the use and disclosure of health information using either "Role-based access" or "User-based access" controls. In this final rule, we do not adopt this requirement.

Comment: We received a large number of comments regarding use of the word "consent." It was pointed out that this could be construed to mean patient consent to the use or disclosure of patient information, which would make this a privacy issue, rather than one of security. Other comments suggested deletion of the requirement in its entirety. We received a comment asking for clarification about the distinction between "Access control" and "Authorizations."

Response: These requirements were intended to address authorization of workforce members and others for the use and disclosure of health information, not patient consent. Upon reviewing the differences between "Access control" and "Authorization control," we found it to be unnecessary to retain "Authorization control" as a separate requirement. Both the access control and the authorization control proposed requirements involved implementation of types of automated access controls, that is, role-based access and user-based access. It can be argued that the process of managing access involves allowing and restricting access to those individuals that have been authorized to access the data. The intent of the proposed authorization control implementation feature is now incorporated in the access

authorization implementation specification under the information access management standard in § 164.308(a)(4). Under the information access management standard, a covered entity must implement, if appropriate and reasonable to its situation, policies and procedures first to authorize a person to access electronic protected health information and then to actually establish such access. These policies and procedures will enable entities to follow the Privacy Rule minimum necessary requirements, which provide when persons should have access to information.

H. Organizational Requirements (§ 164.314)

We proposed that each health care clearinghouse must comply with the security standards to ensure all health information and activities are protected from unauthorized access. If the clearinghouse is part of a larger organization, then unauthorized access by the larger organization must be prevented. We also proposed that parties processing data through a third party would be required to enter into a chain of trust partner agreement, a contract in which the parties agree to electronically exchange data and to protect the transmitted data in accordance with the security standards.

In this final rule, we have adopted the concepts of hybrid and affiliated entities, as previously defined in § 164.504, and now defined in § 164.103, and business associates as defined in § 160.103, to be consistent with the Privacy Rule. General organizational requirements related to affiliated covered entities and hybrid entities are now contained in a new § 164.105. The proposed chain of trust partner agreement has been replaced by the standards for business associate contracts or other arrangements and the standards for group health plans. Consistent with the statute and the policy of the Privacy Rule, this final rule does not require noncovered entities to comply with the security standards.

1. Health Care Clearinghouses

The proposed rule proposed that if a health care clearinghouse were part of a larger organization, it would be required to ensure that all health information pertaining to an individual is protected from unauthorized access by the larger organization; this statement closely tracked the statutory language in section 1173(d)(1)(B) of the Act. Since the point of the statutory language is to ensure that health care information in the possession of a health care clearinghouse is not inappropriately accessed

by the larger organization of which it is a part, this final rule implements the statutory language through the information access management provision of § 164.308(a)(4)(ii)(A).

The final rule, at § 164.105, makes the health care component and affiliated entity standards of the Privacy Rule applicable to the security standards. Therefore, we have not changes those standards substantively. In pertaining to the Privacy Rule, we have simply moved them to a new location in part 164. Any differences between § 164.105 and § 164.504(a) through (d) reflects the addition of requirements specific to the security standards.

The health care component approach was developed in response to extensive comment received principally on the Privacy Rule. See 65 FR 82502 through 82503 and 82637 through 82640 for a discussion of the policy concerns underlying the health care component approach. Since the security standards are intended to support the protection of electronic information protected by the Privacy Rule, it makes sense to incorporate organizational requirements that parallel those required of covered entities by the Privacy Rule. This policy will also minimize the burden of

complying with both rules.

a. Comment: Relative to the following preamble statement (63 FR 43258): "If the clearinghouse is part of a larger organization, then security must be imposed to prevent unauthorized access by the larger organization." One commenter asked what is considered to be "the larger organization." For example, if a clearinghouse function occurs in a department of a larger business entity, will the regulation cover all internal electronic communication, such as e-mail, within the larger business and all external electronic communication, such as e-mail with its owners?

Response: The "larger organization" is the overall business entity that a clearinghouse would be part of. Under the Security Rule, the larger organization must assure that the health care clearinghouse function has instituted measures to ensure only that electronic protected health information that it processes is not improperly accessed by unauthorized persons or other entities, including the larger organization. Internal electronic communication within the larger organization will not be covered by the rule if it does not involve the clearinghouse, assuming that it has designated health care components, of which the health care clearinghouse is one.

External communication must be protected as sent by the clearinghouse, but need not be protected once received.

b. Comment: One commenter asked that the first sentence in § 142.306(b) of the proposed rule, "If a health care clearinghouse is part of a larger organization, it must assure all health information is protected from unauthorized access by the larger organization" be expanded to read, "If a health care clearinghouse or any other health care entity is part of a larger organization . . ."

Response: The Act specifically provides, at section 1173(d)(1)(B), that the Secretary must adopt standards to ensure that a health care clearinghouse, if part of a larger organization, has policies and security procedures to protect information from unauthorized access by the larger organization.

Health care providers and health plans are often part of larger organizations that are not themselves health care providers or health plans. The security measures implemented by health plans and covered health care providers should protect electronic protected health information in circumstances such as the one identified by the commenter. Therefore, we agree with the comment that the requirement should be expanded as suggested by the

commenter. In this final rule, those components of a hybrid entity that are designated as health care components must comply with the security standards and protect against unauthorized access with respect to the other components of the larger entity in the same way as they must deal with separate entities.

2. Business Associate Contracts and Other Arrangements

We proposed that parties processing data through a third party would be required to enter into a chain of trust partner agreement, a contract in which the parties agree to electronically exchange data and to protect the transmitted data. This final rule narrows the scope of agreements required. It essentially tracks the provisions in § 164.502(e) and § 164.504(e) of the Privacy Rule, although appropriate modifications have been made in this rule to the required elements of the contract.

In this final rule, a contract between a covered entity and a business associate must provide that the business associate must--(1) implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity; (2) ensure that

any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate safeguards; (3) report to the covered entity any security incident of which it becomes aware; (4) make its policies and procedures, and documentation required by this subpart relating to such safeguards, available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and (5) authorize termination of the contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract.

When a covered entity and its business associate are both governmental entities, an "other arrangement" is sufficient. The covered entity is in compliance with this standard if it enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of the above-described business associate contract. However, the covered entity may omit from this memorandum the termination authorization required by the business associate contract provisions if this authorization is inconsistent with the statutory obligations of the covered entity or its business associate. If other law (including regulations adopted by

the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of the above-described business associate contract, a contract or agreement is not required. If a covered entity enters into other arrangements with another governmental entity that is a business associate, such arrangements may omit provisions equivalent to the termination authorization required by the business associate contract, if inconsistent with the statutory obligation of the covered entity or its business associate.

If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to receive, create, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of the above-described business associate contract, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by the above described business

associate contract and documents the attempt and the reasons that these assurances cannot be obtained.

We have added a standard for group health plans that parallels the provisions of the Privacy Rule. It became apparent during the course of the security and privacy rulemaking that our original chain of trust approach was both overly broad in scope and failed to address appropriately the circumstances of certain covered entities, particularly the ERISA group health plans. These latter considerations and the solutions arrived at in the Privacy Rule are described in detail in the Privacy Rule at 65 FR 82507 through 82509. Because the purpose of the security standards is in part to reinforce privacy protections, it makes sense to align the organizational policies of the two rules. This decision should also make compliance less burdensome for covered entities than would a decision to have different organizational requirements for the two sets of rules.

Thus, we have added at § 164.314(b) a standard for group health plan that tracks the standard at § 164.504(f) very closely. The purpose of these provisions is to ensure that, except when the electronic protected health information disclosed to a plan sponsor is summary health

information or enrollment or disenrollment information as provided for by § 164.504(f), group health plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained or transmitted to or by the plan sponsor on behalf of the group health plan. The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to implement reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; ensure that any agents, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate safeguards to protect the information; report to the group health plan any security incident of which it becomes aware; and make its policies and procedures and documentation relating to these safeguards available to the Secretary for purposes of determining the group health plan's compliance with this subpart.

a. Comment: Several commenters expressed confusion concerning the applicability of proposed § 142.104 to security.

Response: The proposed preamble included language generally applicable to most of the proposed standards under HIPAA. Proposed § 142.104 concerned general requirements for health plans relative to processing transactions. We proposed that plans could not refuse to conduct a transaction as a standard transaction, or delay or otherwise adversely affect a transaction on the grounds that it was a standard transaction; health information transmitted and received in connection with a transaction must be in the form of standard data elements; and plans conducting transactions through an agent must ensure that the agent met all the requirements that applied to the health plan. Except for the statement that a plan's agent ("business associate" in the final rule) must meet the requirements (which would include security) that apply to the health plan, this proposed section did not pertain to the security standards and was addressed in the Transaction Rule.

b. Comment: The majority of comments concerned proposed rule language stating "the same level of security

will be maintained at all links in the chain . . ." Commenters believed the current language will have an adverse impact on one of the security standard's basic premises, which is scalability. It was requested that the language be changed to indicate that, while appropriate security must be maintained, all partners do not need to maintain the same level of security.

A number of commenters expressed some confusion concerning their responsibility for the security of information once it has passed from their control to their trading partner's control, and so on down the trading partner chain. Requests were made that we clarify that chain of trust partner agreements were really between two parties, and that, if a trading partner agreement has been entered into, any given partner would not be responsible, or liable, for the security of data once it is out of his or her control.

In line with this concern, several commenters were concerned that they would have some responsibility to ensure the level of security maintained by their trading partner.

Several commenters believe a chain of trust partner agreement should not be a security requirement. One

commenter stated that because covered entities must already conform to the regulation requirements, a "chain of trust" agreement does not add to overall security. Compliance with the regulation should be sufficient.

Response: We believe the commenters are correct that the rule as proposed would--(1) not allow for scalability; and (2) would lead an entity to believe it is responsible, and liable, for making sure all entities down the line maintain the same level of security. The confusion here seems to come from the phrase "same level of security." Our intention was that each trading partner would maintain reasonable and appropriate safeguards to protect the information. We did not mean that partners would need to implement the same security technology or measures and procedures.

We have replaced the proposed "Chain of trust" standard with a standard for "Business associate contracts and other arrangements."

When another entity is acting as a business associate of a covered entity, we require the covered entity to require the other entity to protect the electronic protected health information that it creates, receives, maintains or transmits on the covered entity's behalf. The

level of security afforded particular electronic protected health information should not decrease just because the covered entity has made the business decision to entrust a business associate with using or disclosing that information in connection with the performance of certain functions instead of doing those functions itself. Thus, the rule below requires covered entities to require their business associates to implement certain safeguards and take other measures to ensure that the information is safeguarded (see § 164.308(b)(1) and § 164.314(a)(1)).

The specific requirements of § 164.314(a)(1) are drawn from the analogous requirements at 45 CFR 164.504(e) of the Privacy Rule, although they have been adapted to reflect the objectives and context of the security standards. Compare, in particular, 45 CFR 164.504(e)(2)(ii) with § 164.314(a)(1). We have not imported all of the requirements of 45 CFR 164.504(e), however, as many have no clear analog in the security context (see, for example, 45 CFR 164.504(e)(2)(i) regarding permitted and required uses and disclosures made by a business associate). HHS had previously committed to reconciling its security and privacy policies regarding business associates (see 65 FR 82643). The close relationship of many of the

organizational requirements in section § 164.314 with the analogous requirements of the Privacy Rule should facilitate the implementation and coordination of security and privacy policies and procedures by covered entities.

In contrast, when another entity is not acting as a business associate for the covered entity, but rather is acting in the capacity of some other sort of trading partner, we do not require the covered entity to require the other entity to adopt particular security measures, as previously proposed. This policy is likewise consistent with the general approach of the Privacy Rule (see the discussion in the Privacy Rule at 65 FR 82476). The covered entity is free to negotiate security arrangements with its non-business associate trading partners, but this rule does not require it to do so.

A similar approach underlies § 164.314(b) below. These provisions are likewise drawn from, and intended to support, the analogous privacy protections provided for by 45 CFR 164.504(f) (see the discussion of § 164.504(f) of the Privacy Rule at 65 FR 82507 through 82509, and 82646 through 82648). As with the business associate contract provisions, however, they are imported and adapted only to the extent they make sense in the security context. Thus,

for example, the requirement at § 164.504(f)(2)(ii)(C) prohibits the plan documents from permitting disclosure of protected health information to the plan sponsor for employment-related purposes. As this prohibition goes entirely to the permissibility of a particular type of disclosure, it has no analog in § 164.314(b).

c. Comment: Several commenters stated that if security features are determined by agreements established between "trading partners," as stated in the proposed regulations, there should be some guidelines or boundaries for those agreements so that extreme or unusual provisions are not permitted.

Response: This final rule sets a baseline, or minimum level, of security measures that must be taken by a covered entity and stipulates that a business associate must also implement reasonable and appropriate safeguards. This final rule does not, however, prohibit a covered entity from employing more stringent security measures or from requiring a business associate to employ more stringent security measures. A covered entity may determine that, in order to do business with it, a business associate must also employ equivalent measures. This would be a business decision and would not be governed by the provisions of

this rule. Security mechanisms relative to the transmission of electronic protected health information between entities may need to be agreed upon by both parties in order to successfully complete the transmission. However, the determination of the specific transmission mechanisms and the specific security features to be implemented remains a business decision.

d. Comment: Several commenters asked whether existing contracts could be used to meet the requirement for a trading partner agreement, or does the rule require entry into a new contract specific to this purpose. Also, the commenters want to know about those whose working agreements do not involve written contractual agreement: Do they now need to set up formal agreements and incur the additional expense that would entail?

Response: This final rule requires written agreements between covered entities and business associates. New contracts do not have to be entered into specifically for this purpose, if existing written contracts adequately address the applicable requirements (or can be amended to do so).

e. Comment: Several commenters asked whether covered entities are responsible for the security of all individual

health information sent to them, or only information sent by chain of trust partners. They also asked if they can refuse to process standard transactions sent to them in an unsecured fashion. In addition, they inquired if they can refuse to send secured information in standard transactions to entities not required by law to secure the information. One commenter asked if there is a formula for understanding in any particular set of relationships where the ultimate responsibility for compliance with the standards would lie.

Response: Pursuant to the Transactions Rule, if a health plan receives an unsecured standard transaction, it may not refuse to process that transaction simply because it was sent in an unsecured manner. The health plan is not responsible under this rule, for how the transaction was sent to it (unless the transmission was made by a business associate, in which case different considerations apply); however, once electronic protected health information is in the possession of a covered entity, the covered entity is responsible for the security of the electronic protected health information received. The covered entity must implement technical security mechanisms to guard against unauthorized access to electronic protected health information that is transmitted over an electronic

communication network. In addition, the rule requires the transmitting covered entity to obtain written assurance from a business associate receiving the transmission that it will provide an adequate level of protection to the information. For the business associate provisions, see § 164.308(b) and § 164.314(a) of this final rule.

f. Comment: One commenter asked what security standards a vendor having access to a covered entity's health information during development, testing, and repair must meet and wanted to know whether the rule anticipates having a double layer of security compliance (one at the user level and one at the vendor level). If so, the commenter believes this will cause duplication of work.

Response: In the situation described, the vendor would be acting as a business associate. The covered entity must require the business associate to implement reasonable and appropriate security protections of electronic protected health information. This requirement, however, does not impose detailed requirements for how that level of protection must be achieved. The resulting flexibility should permit entities and their business associates to adapt their security safeguards in ways that make sense in their particular environments.

g. Comment: A number of commenters requested sample contract language or models of contracts. We also received one comment that suggested that we should not dictate the contents of contracted agreements.

Response: We will consider developing sample contract language as part of our guideline development.

I. Policies and Procedures and Documentation Requirements (§ 164.316)

We proposed requiring documented policies and procedures for the routine and nonroutine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information. We proposed that the documentation be reviewed and updated periodically.

We have emphasized throughout this final rule the scalability allowed by the security standards. This final rule requires covered entities to implement policies and procedures that are reasonably designed, taking into account the size and type of activities of the covered entity that relate to electronic protected health information, and requires that the policies and procedures must be documented in written form, which may be in electronic form. This final rule also provides that a covered entity may change its policies and procedures at

any time, provided that it documents and implements the changes in accordance with the applicable requirements. Covered entities must also document designations, for example, of affiliation between covered entities (see § 164.105(b)), and other actions, as required by other provisions of the subpart.

1. Comment: One commenter wanted development of written policies regarding such things as confidentiality and privacy rights for access to medical records, and approval of research by a review board when appropriate.

Response: These issues are covered in the Privacy Rule (65 FR 82462) (see, in particular, § 164.512(i), § 164.524, and § 164.530(i)).

2. Comment: One commenter asked if standards will override agreements that require others to maintain hardcopy documentation (for example, signature on file) and no longer require submitters to maintain hardcopy documentation.

Response: The security standards will require a minimum level of documentation of security practices. Any agreements between trading partners for the exchange of electronic protected health information that impose additional documentation requirements will not be

overridden by this final rule.

3. Comment: One commenter stated that there should be a requirement to document only applications deemed necessary by an applications and data criticality assessment.

Response: Electronic protected health information must be afforded security protection under this rule regardless of what application it resides in. The measures taken to protect that information must be documented.

4. Comment: One commenter asked how detailed the documentation must be. Another commenter asked what "kept current" meant.

Response: Documentation must be detailed enough to communicate the security measures taken and to facilitate periodic evaluations pursuant to § 164.308(a)(8). While the term "current" is not in the final rule, this concept has been adopted in the requirement that documentation must be updated as needed to reflect security measures currently in effect.

5. Comment: We received one comment concerning review and updating of implementing documentation suggesting that "periodically" be changed to "at least annually."

Response: We believe that the requirement should remain as written, in order to allow individual entities to establish review and update cycles as deemed necessary. The need for review and update will vary dependent upon a given entity's size, configuration, environment, operational changes, and the security measures implemented.

J. Compliance Dates for Initial Implementation (§ 164.318)

We proposed that how the security standard would be implemented by each covered entity would be dependent upon industry trading partner agreements for electronic transmissions. Covered entities would be able to adapt the security matrix to meet business needs. We suggested that requirements of the security standard may be implemented earlier than the compliance date. However, we would require implementation to be complete by the applicable compliance date, which is 24 months after adoption of the standard, and 36 months after adoption of the standard for small health plans, as provided by the Act. In the proposed rule, we suggested that an entity choosing to convert from paper to standard EDI transactions, before the effective date of the security standard, consider implementing the security standard at the same time.

In this final rule the dates by which entities must be in compliance with the standards are called "compliance dates," consistent with our practice in the Transactions, Privacy, and Employer Identifier Rules. Section 164.318 in this final rule is also organized consistent with the format of those rules. The substantive requirements, which are statutory, remain unchanged.

Many of the comments received concerning effective dates and compliance dates, including the compliance dates for modifications of standards, were addressed in the Transactions Rule. Those that were not addressed in that publication are presented below.

1. Comment: A number of commenters expressed support for the effective dates of the rules and stated that they should not be delayed. In contrast, one commenter stated that we should delay this rule to allow for an open consensus building debate to occur concerning security. One commenter asked that the rule be delayed until after implementation of the ICD-CM changes.

A number of comments were received expressing the opinion that the security regulation should not be published until either the Congress has enacted legislation governing standards with respect to the privacy of

individually identifiable health information, or the Secretary of HHS has promulgated final regulations containing these standards. One commenter stated, "we find ourselves in the difficult position of reacting to proposed rules setting the standards for how information should be physically and electronically protected, without having reached agreement on the larger issues of consent for and disclosure of individual medical information."

Response: The effective date of the final rule is 60 days after this final rule is published in the **Federal Register**. The statute sets forth the compliance dates for the standards. Covered entities must comply with this final rule no later than 24 months (36 months for small plans) after the effective date.

The final Privacy Rule has already been published. We note that numerous comments concerning the timing of the adoption of privacy and security standards were also received in the privacy rulemaking and are discussed in the Privacy Rule at 65 FR 82752.

2. Comment: One commenter asked that proposed § 142.312 be rewritten to separate the effective dates for the Security Rule and the Transactions Rule.

Response: The proposed rule incorporated general

language applicable to all the proposed Administrative Simplification standards. Language concerning standards other than Security is not included in § 164.318. Because this final rule is adopted after the Transactions Rule was adopted, the compliance dates for the security standards differ from those for the transactions standards. Comments concerning general effective dates were addressed in the Transactions Rule. Comments specific to the security standards are addressed here.

3. Comment: Several commenters suggested that we not allow early implementation of the Security Rules. A number of others asked that we allow, but not require, early implementation by willing trading partners. Another commenter suggested that early implementation by willing trading partners be allowed as long as the data content transmitted is equal to that required by statute. Another commenter requested that it be stipulated that entities cannot implement less than 1 year from the date of this final rule and then only after successful testing, and that a "start testing by" date be defined.

Response: Whether or not to implement before the compliance date is a business decision that each covered entity must make. Moreover, the vast majority of the

standards address internal policies and procedures that can be implemented at any time without any impact on trading partners.

4. Comment: One commenter asked us to establish a research site or test laboratory for a trial implementation.

Response: The concept of a "trial implementation" that would have widespread relevance is inconsistent with our basic principles of flexibility, scalability, and technology-neutrality.

5. Comment: One commenter stated that the 2-year time frame for implementation of a contingency plan is too short for health plans that serve multiple regions of the country.

Response: The Congress mandated that entities must be in compliance 2 years from the initial standard's adoption date (3 years for small plans).

K. Appendix

The proposed rule contained three addenda. Addendum 1 set out in matrix form the proposed requirements and related implementation features of the proposed rule. Addendum 2 set out in list form a glossary of terms with citations to the sources of those terms. Addendum 3

identified and mapped areas of overlap in the proposed security standard and implementation features.

This final rule retains only the first proposed addendum, the matrix, as an appendix, that is modified to reflect the changes in the administrative, physical, and technical safeguard portions of the rule below. Numerous terms in the glossary now appear in the rule below, typically (but not always) as definitions.

1. Comment: Over two-thirds of the comments received on this topic asked that the matrix be incorporated into the final rule. One commenter asked that a simplified version be made part of the final rule. Six commenters wanted it kept in this final rule as an addendum. One commenter stated that it should be in an appendix to the rule, while others stated that it should not be included in this final rule.

Response: Since a significant majority of commenters requested retention of the matrix, it has been incorporated into this final rule as an appendix. The matrix displays, in tabular form, the administrative, physical, and technical safeguard standards and relating implementation specifications described in this final rule in § 164.308, § 164.310, and § 164.312. It should be noted that the

requirements of § 164.105, § 164.314, and § 164.316 are not presented in the matrix.

2. Comment: A large majority of commenters stated that the glossary located in Addendum 2 of the proposed rule should be included as part of the final rule. Several commenters asked that it be incorporated into the definitions section of the final rule. One commenter stated that the glossary should not be part of this final rule.

Response: The terms defined in the glossary in Addendum 2 of the proposed rule are found throughout this final rule, either as part of the text of § 164.306 through § 164.312 or under § 164.304, as appropriate. We included only terms relevant to the particular standards and implementation specifications being adopted.

3. Comment: Several commenters requested that the mapped matrix located in Addendum 3 of the proposed rule be included in this final rule, either as part of the rule or as an addendum, while others stated that it should not be part of this final rule. Several commenters cited items to be added to the mapped matrix.

Response: The mapped matrix was merely a snapshot of current standards and guidelines that the implementation

team was able to obtain for review during the development of the security and electronic signature requirements and was provided in the proposed rule as background material. Since this matrix has not been fully populated or kept up-to-date, it is not being published as part of this final rule. Where relevant, we do reference various standards and guidelines indicated in the matrix in this preamble.

L. Miscellaneous Issues

1. Preemption

The statute requires generally that the security standards supersede contrary provisions of State law including State law requiring medical or health plan records to be maintained or transmitted in written rather than electronic formats. The statute provides certain exceptions to the general rule; section 1178(a)(2) of the Act identifies conditions under which an exception applies. The proposed rule did not provide for a process for making exception determinations; rather, a process was proposed in the privacy rulemaking and was adopted with the Privacy Rule (see part 160, subpart B). This process applies to exception determinations for all of the Administrative Simplification rules, including this rule.

a. Comment: Several commenters stated that the proposed rule does not include substantive protections for the privacy rights of patients' electronic medical records, while the rule attempts to preempt State privacy laws with respect to these records. Comments stated that, by omitting a clarification of State privacy law applicability, the proposed rule creates confusion. They believe that the rule must contain express and specific exemptions of State laws with respect to medical privacy.

Response: The Privacy Rule establishes standards for the rights of patients in regard to the privacy of their medical records and for the allowable uses and disclosures of protected health information. The identified concerns were discussed in the Privacy Rule (see 65 FR 82587 through 82588). The security standards do not specifically address privacy but will safeguard electronic protected health information against unauthorized access or modification.

b. Comment: One commenter asked how these regulations relate to confidentiality laws, which vary from State to State.

Response: It is difficult to respond to this question in the abstract without the benefit of reference to a specific State statute. However, in general, these

security standards will preempt contrary State laws. Per section 1178(a)(2) of the Act, this general rule would not hold if the Secretary determines that a contrary provision of State law is necessary for certain identified purposes to prevent fraud and abuse; to ensure appropriate State regulation of insurance and health plans; for State reporting on health care delivery costs; or if it addresses controlled substances. See 45 CFR part 160 subpart B. In such case, the contrary provision of State law would preempt a Federal provision of these security standards. State laws that are related but not contrary to this final rule, will not be affected.

Section 1178 of the Act also limits the preemptive effect of the Federal requirements on certain State laws other than where the Secretary makes certain determinations. Section 1178(b) of the Act provides that State laws for reporting of disease and other conditions and for public heath surveillance, investigation, or intervention are not invalidated or limited by the Administrative Simplification rules. Section 1178(c) of the Act provides that the Federal requirements do not limit States' abilities to require that health plans report or provide access to certain information.

c. Comment: Several commenters stated that allowing State law to establish additional security restrictions conflicts with the purpose of the Federal rule and/or would make implementation very difficult. One commenter asked for clarification as to whether additional requirements tighter than the requirements outlined in the proposed rule may be imposed.

Response: The general rule is that the security standards in this final rule supersede contrary State law. Only where the Secretary has granted an exception under section 1178(a)(2)(A) of the Act, or in situations under section 1178(b) or (c) of the Act, will the general rule not hold true. Covered entities may be required to adhere to stricter State-imposed security measures that are not contrary to this final rule.

2. Enforcement

The proposed rule did not contain specific enforcement provisions. This final rule likewise does not contain specific enforcement provisions; it is expected that enforcement provisions applicable to all Administrative Simplification rules will be proposed in a future rulemaking.

a. Comment: One commenter voiced support for the

proposed rule's approach. Another stated that the process is poorly defined. One commenter stated that fines should be eliminated, or the scope of activity subject to fines should be more narrowly defined.

While a number of commenters were of the opinion that HHS must retain enforcement responsibility, stating that it would be unconstitutional to give it to a private entity, several others stated that it may not be practical for HHS to retain the responsibility for determining violations and imposing penalties specified by the statute. A concern was voiced over HHS's ability to fairly and consistently apply the rules due to budget constraints. Several commenters support industry solutions to enforcement with some level of government involvement. One commenter recommended a single audit process using accrediting bodies already in place. Another stated that entities providing accreditation services should not be involved in enforcement as this would result in a conflict of interest.

Clarification was requested, including the use of examples, concerning what constitutes a violation, and how a penalty applies to a "person." Commenters asked if the term "person" referred to the people responsible for the system and how penalties would apply to corporations and

other entities.

Response: It is expected that enforcement of HIPAA standards will be addressed in regulations to be issued at a later date.

b. Comment: Several commenters stated that enforcement of the security standards will be arbitrarily delegated to private businesses that compete with physicians and with each other.

Response: These comments are premature for the reasons stated above.

3. Comment Period

The comment period on the proposed rule was 60 days.

Comment: We received comments suggesting that significant changes to the standards could occur in the final rule as a result of changes made in response to comments. The commenter believes such changes could adversely affect payers and providers, and suggested that the rule should be republished as a proposed rule with a new comment period to allow additional comments concerning any changes. A "work-in-progress" approach was also suggested, to give all stakeholders time to read, analyze, and comment upon evolving versions of a particular proposed rule.

Response: We have not accepted these suggestions. The numerous comments received were thoughtful, analytical, detailed, and addressed every area of the proposed rule. This response to the proposed rule indicates that the public had ample time to read, analyze, and comment upon the proposed rule. If we were to treat the rule as a "work-in-progress" and issue evolving versions, allowing for comments to each version, we would never implement the statute and achieve administrative simplification as directed by the Congress.

M. Proposed Impact Analysis

The preamble to the Transactions Rule contains comments and responses on the impact of all the administrative simplification standards in general except privacy. Comments and responses specific to the relative impact of implementing this final rule are presented below.

a. Comment: Several commenters stated that the proposed security standards are complex, costly, administratively burdensome, and could result in decreased use of EDI. One commenter stated that this rule runs counter to the explicit intent of Administrative Simplification that requires, "any standard adopted under this part shall be consistent with the objective of

reducing the administrative costs of providing and paying for health care."

Several commenters expressed concern that there was no cost benefit analysis provided for these proposed regulations, stating that, faced with increasingly limited resources, it is essential that a security standards cost/benefit analysis for all health care trading partners be provided. Another said an independent cost estimate by the General Accounting Office (GAO) should be performed on these rules and HHS cost estimates should be publicized for comparison purposes.

Still another commenter stated that HHS must provide accurate public sector implementation cost figures and provide funds to offset the cost burden.

One commenter asked for cost benefit evaluations to understand the relationship between competing technologies, levels of security and potential threats to be guarded against. These would demonstrate the costs and the benefits to be gained for both large and small organizations and would provide an understanding of how the levels of security vary by organization size and what the inducements and support available to facilitate adoption are. One commenter suggested that we establish a workgroup

to more fully assess the costs and provide Federal funds to offset implementation costs.

One commenter noted a seeming disconnect between two statements in the preamble. Section A, Security standards, states, "no individual small entity is expected to experience direct costs that exceed benefits as a result of this rule." In contrast, section E, Factors in establishing the security standards reads, "We cannot estimate the per-entity cost of implementation because there is no information available regarding the extent to which providers', plans', and clearinghouses' current security practices are deficient."

Response: We are unable to estimate, of the nation's 2 million-plus health plans and 1 million-plus providers that conduct electronic transactions, the number of entities that would require new or modified security safeguards and procedures beyond what they currently have in place. Nor are we able to estimate the number of entities that neither conduct electronic transactions nor maintain individually identifiable electronic health information but may become covered entities at some future time. As we are unable to estimate the number of entities and what measures are or are not already in place, or what

specific implementation will be chosen to meet the requirements of the regulation, we are also unable to estimate the cost to those entities.

However, the use of electronic technology to maintain or transmit health information results in many new and potentially large risks. These risks represent expected costs, both monetary and social. Leaving risk assessment up to individual entities will minimize the impact and ensure that security effort is proportional to security risk.

As discussed earlier, the security requirements are both scalable and technically flexible. We have made significant changes to this final rule, reducing the number of required implementation features and providing for greater flexibility in satisfaction of the requirements. In other words, we have focused more on what needs to be done and less on how it should be accomplished.

We have removed the statement regarding the extent of costs versus benefits for small entities.

b. Comment: One commenter stated that on page 43262 of the proposed rule, it indicate that complexity of conversion to the security standards would be affected by the choice to use a clearinghouse. The commenter stated

that this choice would have little effect on implementation of security standards. Another commenter stated that the complexity (and cost) of the conversion to meet the security standards is affected by far more than just the "volume of claims health plans process electronically and the desire to transmit the claims or to use the services of a VAN or clearinghouse" as is stated on page 43262. Because the security standards apply to internal systems as well as to transactions between entities, a number of additional factors must be considered, for example, modification of existing security mechanisms, legacy systems, architecture, and culture.

Response: We agree. We have modified the Regulatory Impact Analysis section to take into account that there are other factors involved, such as the architecture and technology limitations of existing systems.

c. Comment: One commenter stated that States will need 90 percent funding of development and implementation, without the burden of an advanced planning documents requirement, from us for this costly process to succeed. Any new operational obligation should be 100 percent funded. Also human resource obligations will be significant. Some States believe they will have difficulty

obtaining the budget funds for the State share of the costs. State Medicaid agencies, as purchasers, may also face paying the implementation costs of health care providers, clearinghouses, and health plans in the form of higher rates.

Response: The statute does not authorize any new or special funding for implementation of the regulations. Medicaid system changes, simply because they are "HIPAA related" do not automatically qualify for 90 percent Federal funding participation. As with any systems request, the usual rules will be applied to determine funding eligibility for State HIPAA initiatives. Nevertheless, HHS recognizes that there are significant issues regarding the funding and implementation of HIPAA by Medicaid State agencies, and intends to address them through normal channels of communication with States.

d. Comment: One commenter stated that the proposed rule does not establish how the security standards will contribute to reduced cost for providers. One commenter expected the unintended result of this regulation will be impediment of EDI growth and perhaps even a decline in EDI use by providers. Another stated that the proposed rule actively discourages physician EDI participation by

suggesting a fallback to paper processing for those unable to meet the cost of highly complex security compliance.

Response: Ensuring the integrity of an electronic message, its delivery to the correct person, and its confidentiality must be an integral part of conducting electronic commerce. We believe that the consistent application of the measures provided in this rule will actually encourage use of EDI because it will provide increased confidence in the reliability and confidentiality of health information to all parties involved. Also, the implementation of these security requirements will reduce the potential overall cost of risk to a greater extent than additional security controls will increase costs. Put another way, the potential cost of not reasonably addressing security risks could substantially exceed the cost of compliance.

e. Comment: One commenter stated that the implementation impact of the technical safeguards is clearly understated for physicians who use digitally-based equipment that has been in place for some time. The commenter believes that the rule will likely have greatest impact on the installed base of digital systems, including imaging modalities and other medical devices that store or

transmit patient information because software for legacy systems will likely require retrofitting or replacement to come into compliance. The commenter believes that this is a negative impact and would outweigh any benefits derived from the potential risk of security breaches. The commenter recommended compliance for digital imaging devices be extended by an additional 3 years to allow time to upgrade systems and defray the associated costs.

Response: Compliance dates for the initial implementation of the initial standards are statutorily prescribed; therefore, we are unable to allow additional time outside of the statutory timeframes for compliance.

f. Comment: A commenter stated that, as a new regulatory mandate, HIPAA costs must be factored into any base year calculations for the proposed prospective payment system. Without an adjustment, this will be another regulatory mandate that comes at the cost of patient care.

Response: Costs included in the prospective payment system are legislatively mandated. The Congress did not direct the inclusion of HIPAA costs into the system, so they are not included. However, the Department believes that the HIPAA standards will provide savings to the provider community over the next 10 years.

g. Comment: One commenter suggested that we include requirements for how a compliant business could dually operate--(1) in a HIPAA compliant manner; and (2) in their former noncompliant manner in order to accommodate doing business with other organizations that are not yet compliant.

Response: The statute imposes a 2-year implementation period between the adoption of the initial standards and the date by which covered entities (except small health plans) must be in compliance. An entity may come into compliance at any point in time during the 2 years. Therefore, the rule does not require a covered entity to comply before the established compliance date. Those entities that come into compliance before the 2-year deadline should decide how best to deal with entities that are not yet compliant. Further, we note that, generally speaking, compliance by a covered entity with these security rules will not hinge on compliance by other entities.

h. Comment: One commenter stated that privacy legislation could impose significant changes to written policies and procedures on authorization, access to health information, and how sensitive information is disclosed to

others. The commenter believes these changes could mean the imposition of security requirements different from those contained in the proposed rule, and money spent complying with the security provisions could be ill spent if significant new requirements result from the privacy legislation.

Response: The privacy standards at subpart E of 42 CFR part 164 are now in effect, and this final rule is compatible with them. If, in the future, the Congress passes a law whose provisions differ from these standards, the standards would have to be modified.

i. Comment: One commenter stated that the private sector should develop educational tools or models in order to assist physicians, other providers, and health plans to comply with the security regulations.

Response: We agree. The health care industry is striving to do this. HHS is also considering provider outreach and education activities.

IV. Provisions of the Final Regulation

We have made the following changes to the provisions of the August 12, 1998 proposed rule. Specifically, we have--

- Changed the CFR part from 142 to 164.
- Removed information throughout the document pertaining to electronic signature standards. Electronic signature standards will be published in a separate final rule.
- Replaced the word "requirement," when referring to a standard, with "standard." Replaced "Implementation feature" with "Implementation specification."
- Made minor modifications to the text throughout the document for purposes of clarity.
- Modified numerous implementation features so that they are now addressable rather than mandatory.
- Removed the word "formal" when referring to documentation.
- Revised the phrase "health information pertaining to an individual" to "electronic protected health information."
- Added the following definitions to § 160.103:

"Disclosure," "Electronic protected health information," "Electronic media," "Organized health care arrangement," and "Use."

- Removed proposed § 142.101 as this information is conveyed in § 160.101 and § 160.102 of the Privacy Rule (65 FR 82798). Removed proposed § 142.102 as it is redundant.

- Removed the following definitions from proposed § 142.103 since they are pertinent to other administrative simplification regulations and are defined elsewhere: code set, health care clearinghouse, health care provider, health information, health plan, medical care, small health plan, standard, and transaction.

- Moved the following definitions from § 164.501 to § 164.103 (proposed § 142.103): " "Plan sponsor" and "Protected health information." Added definitions of "Covered functions" and "Required by law."

- Removed proposed § 142.104, "General requirements for health plans," and proposed § 142.105, "Compliance using a health care clearinghouse," since these sections are not pertinent to the security standards.

- Removed proposed § 142.106, "Effective dates of a modification to a standard or implementation

specification," since this information is covered in the "Standards for Electronic Transactions" final rule (65 FR 50312).

- Moved proposed § 142.302 to § 164.302. Changed the section heading from "Applicability and scope" to "Applicability." Modified language to state that covered entities must comply with the security standards.

- Moved proposed § 142.304 to § 164.304. Modified language to remove definitions of words and concepts not used in this final rule: "Access control," "Contingency plan," "Participant," "Role-based access control," "Token," and "User-based access."

- Moved proposed § 142.304 to § 164.304. Modified language to add definitions requested by commenters; previously published in Addendum 2 but not in the draft regulation itself; or necessitated by the change of scope to electronic protected health information and alignment with the Privacy Rule to include: "Administrative safeguards," "Availability," "Confidentiality," "Data," "Data authentication Code," "Integrity," "Electronic protected health information," "Facility," "Information System," "Security or security measures," "Security incident," "Technical safeguards," "User," and

"Workstation."

- Moved definitions related to privacy from § 164.504 to new § 164.103: "Common control," "Common ownership," "Health care component," "Hybrid entity."

- Moved proposed § 142.306, "Rules for the security Standard," to § 164.306. Modified language to more clearly state the general requirements of the final rule relative to the standards and implementation specifications contained therein. Retitled the section as "Security standards: General Rules."

- Moved proposed § 142.308 to § 164.308. Where this section was proposed to contain all of the security standards in paragraphs (a) through (d), it now encompasses the Administrative safeguards.

- Moved and reorganized proposed § 142.308(a) through (d) requirements to § 164.308, § 164.310, and § 164.312.

- Moved proposed § 142.308(a)(1), "Certification," to § 164.308(a)(8). Modified language to indicate both technical and nontechnical evaluation is involved and renamed "Evaluation".

- Moved proposed § 142.308(a)(2), "Chain of trust," to

§ 164.308(b)(1), renamed to "Business associate contracts and other arrangements," and revised language to redefine who must enter into a contract under this rule for the protection of electronic protected health information.

- Moved proposed § 142.308(a)(3), "Contingency plan," to § 164.308(a)(7)(i). Modified language to state that two implementation specifications, "Applications and data criticality analysis" and "Testing and revision procedures," are addressable.

- Removed "Formal mechanism for processing records" (proposed § 142.308(a)(4)) since this requirement was determined to be in part intrusive into business functions and in part redundant.

- Moved proposed § 142.308(a)(5), "Information access control," to § 164.308(a)(4)(i) and renamed as "Information access management." Removed the word "formal" from description. Modified language to state that two implementation specifications ("Access Authorization" and Access Establishment and Modification") are addressable.

- Moved proposed § 142.308(a)(6), "Internal audit," to § 164.308(a)(1)(ii)(D) as an implementation specification under the "Security management process" standard since this was determined to be a more logical

placement of this item. Retitled, for clarity, "Information system activity review."

- Moved proposed § 142.308(a)(7), "Personnel security," to § 164.308(a)(3)(i) and retitled "Workforce security." Modified language to state that implementation specifications are addressable.

- Combined proposed § 142.308(a)(7)(i), and § 142.308(a)(7)(iii) ("Assuring supervision of maintenance personnel by an authorized, knowledgeable person" and "Assuring that operations and maintenance personnel have proper access authorization,") under § 164.308(a)(3)(ii)(A) and renamed to "Authorization and/or supervision." Modified description for clarity.

- Moved proposed § 142.308(a)(7)(iv), "Personnel clearance procedure," to § 164.308(a)(3)(ii)(B), renamed to "Workforce clearance procedure," and modified description for clarity.

- Removed proposed § 142.308(a)(7)(v), "Personnel security policies and procedures," as this feature was determined to require redundant effort.

- Removed proposed § 142.308(a)(7)(vi), "Security awareness training." Information concerning this subject has been incorporated under § 164.308(a)(5)(i), "Security

awareness and training."

- Removed proposed § 142.308(a)(8), "Security configuration management," and all implementation features, except "Documentation" (hardware and/or software installation, Inventory, Security testing, and Virus checking), since this requirement was determined to be redundant. "Documentation" has been made a discrete standard at § 164.316.

- Moved proposed § 142.308(a)(9), "Security incident procedures," to § 164.308(a)(6)(i) and reworded for clarity. Combined "Report procedures" and "Response procedures" features into a single required implementation specification, named "Response and Reporting" at § 164.308(a)(6)(ii).

- Moved proposed § 142.308(a)(10), "Security management process," to § 164.308(a)(1).

- Moved proposed § 142.308(a)(10)(i), "Risk analysis," to § 164.308(a)(1)(ii)(A).

- Moved proposed § 142.308(a)(10)(ii), "Risk management," to § 164.308(a)(1)(ii)(B).

- Moved proposed § 142.308(a)(10)(iii), "Sanction policy," to § 164.308(a)(1)(ii)(C).

- Removed proposed § 142.308(a)(10)(iv), "Security policy," since this requirement was determined to be redundant.

- Moved proposed § 142.308(a)(11), "Termination," to § 164.308(a)(3)(ii)(C) as an addressable implementation specification under the "Workforce security" standard, and renamed as "Termination procedures". Removed "Termination" implementation features (changing locks, removal from access lists, removal of user accounts, turning in of keys, tokens, or cards) since these were determined to be too specific.

- Moved proposed § 142.308(a)(12), "Training," to § 164.308(a)(5)(i) and renamed as "Security awareness and training." Language modified to incorporate all training information under this one standard. Revised and made addressable all implementation specifications under this standard.

- Moved proposed § 142.308(b), "Physical safeguards to guard data integrity, confidentiality and availability," to § 164.310 and renamed as "Physical safeguards." Removed specific reference to locks and keys.

- Moved proposed § 142.308(b)(1), "Assigned security responsibility requirement," to § 164.308(a)(2) since this

has been determined to be an administrative procedure. Modified language to clarify that responsibility could be assigned to more than one individual.

- Moved proposed § 142.308(b)(2), "Media controls," to § 164.310(d)(1) and renamed as "Device and media controls." Removed the word "formal." Added "Media re-use" as a required implementation specification at § 164.310(d)(2)(ii).

- Removed proposed § 142.308(b)(2)(i), "Access control," implementation feature as it was determined to be redundant.

- Moved proposed § 142.308(b)(2)(ii), "Accountability" implementation feature to § 164.310(d)(2)(iii), and made it an addressable implementation specification.

- Combined proposed § 142.308(b)(2)(iii), "Data backup," implementation feature with proposed § 142.308(b)(2)(iv), "Data storage" implementation feature, renamed as "Data backup and storage", moved to § 164.310(d)(2)(iv), and made it an addressable implementation specification.

- Moved proposed § 142.308(b)(2)(v), "Data disposal," implementation feature to § 164.310(d)(2)(i) and made it a required implementation specification.

- Moved proposed § 142.308(b)(3),"Physical access controls," to § 164.310(a)(1) and renamed as "Facility access controls." Removed word "formal."

- Moved proposed § 142.308(b)(3)(i), "Disaster recovery," implementation feature to § 164.310(a)(2)(i). It is now part of the "Contingency operations" implementation specification.

- Moved proposed § 142.308(b)(3)(ii), "Emergency mode operations," implementation feature to § 164.310(a)(2)(i). It is now part of the "Contingency operations" implementation specification.

- Removed proposed § 142.308(b)(3)(iii), "Equipment control (into and out of site)," as this information is now covered under § 164.310(d)(1), "Device and media controls."

- Moved proposed § 142.308(b)(3)(iv), "A facility security plan," to § 164.310(a)(2)(ii).

- Moved proposed § 142.308(b)(3)(v), "Procedure for verifying access authorizations," to § 164.310(a)(2)(iii) and renamed as "Access control and validation procedures." Removed the word "formal" from text.

- Moved proposed § 142.308(b)(3)(vi), "Maintenance records," to § 164.310(a)(2)(iv).

- Moved proposed § 142.308(b)(3)(vii), "Need to know procedures for personnel access," to § 164.310(a)(2)(iii) and renamed as "Access control and validation procedures."

- Moved proposed § 142.308(b)(3)(viii), "Procedures to sign in visitors and provide escort, if appropriate," to § 164.310(a)(2)(iii) and renamed as "Access control and validation procedures."

- Moved proposed § 142.308(b)(3)(ix), "Testing and revision," to § 164.310(a)(2)(iii) and renamed as "Access control and validation procedures."

- Moved proposed § 142.308(b)(4), "Policy and guidelines on workstation use," to § 164.310(b) and renamed as "Workstation use."

- Moved proposed § 142.308(b)(5), "Secure work station location," to § 164.310(c) and renamed as "Workstation security."

- Removed proposed § 142.308(b)(6), "Security awareness training," as a separate requirement. This requirement has been incorporated under § 164.308(a)(5)(i), "Security awareness and training."

- Combined and moved proposed § 142.308(c) and § 142.308(d), "Technical security services to guard data

integrity, confidentiality and availability" and "Technical security mechanisms," to § 164.312 and renamed as "Technical safeguards."

- Removed proposed § 142.308(c)(1) since it is no longer pertinent.
- Moved proposed § 142.308(c)(1)(i), "Access control," to § 164.312(a)(1).
- Moved proposed § 142.308(c)(1)(i)(A), "Procedure for emergency access," to § 164.312(a)(2)(ii), and renamed as "Emergency access procedures."
- Removed proposed § 142.308(c)(1)(i)(B).
- Removed proposed § 142.308(c)(1)(i)(B)(1), "Context-based access," § 142.308(c)(1)(i)(B)(2), "Role-based access," and § 142.308(c)(1)(i)(B)(3), "User-based access," since these features were deemed too specific and were perceived as the only options permissible.
- Moved proposed § 142.308(c)(1)(i)(C), "Optional use of encryption," to § 164.312(a)(2)(iv) and retitled "Encryption and decryption."
- Moved proposed § 142.308(c)(1)(ii), "Audit controls," to § 164.312(b).
- Removed proposed § 142.308(c)(1)(iii),

"Authorization control," and all implementation features (Role-based access, User-based access) since this function has been incorporated into § 164.308(a)(4), "Information access management."

- Moved proposed § 142.308(c)(1)(iv), "Data authentication," to § 164.312(c)(1), and retitled as "Integrity." Reworded part of description and placed in § 164.312(c)(2), "Mechanism to authenticate data," a new, addressable implementation specification. Removed reference to double keying.

- Moved proposed § 142.308(c)(1)(v), "Entity authentication," to § 164.312(d) and retitled as "Person or entity authentication."

- Moved proposed § 142.308(c)(1)(v)(A), "Automatic logoff," to § 164.312(a)(2)(iii).

- Moved proposed § 142.308(c)(1)(v)(B), "Unique user identification," to § 164.312(a)(2)(i).

- Removed proposed § 142.308(c)(1)(v)(C) since text is no longer pertinent.

- Removed proposed § 142.308(c)(1)(v)(C)(2), "Password," as too specific.

- Removed proposed § 142.308(c)(1)(v)(C)(3), "PIN," as

too specific.

- Removed proposed § 142.308(c)(1)(v)(C)(4), "Telephone callback," as too specific.

- Removed proposed § 142.308(c)(1)(v)(C)(5), "Token," as too specific.

- Removed proposed § 142.308(c)(2), as no longer relevant.

- Moved proposed § 142.308(d)(1), "Communications or network controls," to § 164.312(e)(1) and renamed as "Transmission security."

- Removed proposed § 142.308(d)(1)(i), since it is no longer pertinent.

- Moved proposed § 142.308(d)(1)(i)(A), "Integrity controls," to § 164.312(e)(2)(i) and reworded for clarity.

- Removed proposed § 142.308(d)(1)(i)(B), "Message authentication," since this subject is now covered under § 164.312(e)(2)(i), "Integrity controls."

- Removed proposed § 142.308(d)(1)(ii) text since it is no longer pertinent.

- Removed proposed § 142.308(d)(1)(ii)(A), "Access controls."

- Moved proposed § 142.308(d)(1)(ii)(B), "Encryption,"

to § 164.312(e)(2)(ii) and reworded to enhance flexibility and scalability.

- Removed proposed § 142.308(d)(2) text regarding: "Network controls," and all implementation features ("Alarm," "Audio trail," "Entity authentication," "Event reporting").

- Removed proposed § 142.310, "Electronic signature," and all subheadings. This section will be issued as a separate future regulation.

- Moved proposed § 142.310 "Electronic signature Standard," to § 164.310. Where this section was proposed to contain the electronic signature standard, it now encompasses the "Physical safeguards."

- Moved proposed § 142.312, "Effective date of the implementation of the security and electronic signature standards," to § 164.318 and retitled as "Compliance dates for the initial implementation of the security standards." Reworded and retitled subsections.

- Added § 164.105, "Organizational requirements," with two standards, "Health care component and "Affiliated covered entities" with related implementation specifications.

- Added § 164.310(d)(2)(ii), "Media re-use procedures," implementation specification.
- Added § 164.312, "Technical safeguards," encompassing the combined technical services and technical mechanisms standards (proposed § 142.308 (c) and (d)).
- Added § 164.314, "Organizational requirements."
- Added § 164.314(a)(1), "Business associate contracts or other arrangements" standard and related implementation specifications.
- Added § 164.314(b)(1), "Requirements for group health plans" standard and related implementation specifications.
- Added § 164.316, "Policies and procedures and documentation requirements."
- Added § 164.316(a), "Policies and procedures" standard.
- Added § 164.316(b)(1), "Documentation" standard and related implementation specifications.
- Added § 164.318, "Compliance dates for the initial implementation of the security standards."
- Renamed Addendum 1 as Appendix A.
- Removed Addendum 2. Definitions of terms used in

this final rule are now incorporated into § 164.103 and § 164.304, or within the rule itself.

- Removed Addendum 3.

V. Collection of Information Requirements

Under the Paperwork Reduction Act of 1995 (PRA), we are required to provide 30-day notice in the **Federal Register** and solicit public comment before a collection of information requirement is submitted to the Office of Management and Budget (OMB) for review and approval. In order to fairly evaluate whether an information collection should be approved by OMB, section 3506(c)(2)(A) of the Paperwork Reduction Act of 1995 (PRA) requires that we solicit comment on the following issues:

- The need for the information collection and its usefulness in carrying out the proper functions of our agency.

- The accuracy of our estimate of the information collection burden.

- The quality, utility, and clarity of the information to be collected.

- Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

As discussed below, we are soliciting comment on the recordkeeping requirements, as referenced in § 164.306, § 164.308, § 164.310, § 164.314, and § 164.316 of this document.

§ 164.306 Security standards: General rules.

Under paragraph (d), a covered entity must, if implementing the implementation specification is not reasonable and appropriate, document why it would not be reasonable and appropriate to implement the implementation specification.

We estimate that 75,000 entities will be affected by this requirement and that they will have to create documentation 3 times for this requirement. We estimate each instance of documentation will take .25 hours, for a one-time total burden of 56,250 hours.

§ 164.308 Administrative safeguards.

Under this section, a covered entity must document known security incidents and their outcomes.

We estimate that there will be 50 known incidents annually and that it will take 8 hours to document this requirement, for an annual burden of 400 hours.

This section further requires that each entity have a contingency plan, with specified components.

We estimate that there will be 60,000 entities affected by this requirement and that it will take each entity 8 hours to comply, for a total one-time burden of 480,000 hours.

This section also requires that the written contract or other arrangement with a business associate document the satisfactory assurances that the business associate will appropriately safeguard the information through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

We believe that the burden associated with this requirement is not subject to the PRA. It is good business practice for entities to document their arrangements via written contracts and as such is usual and customary among the entities subject to them. A burden associated with a requirement conducted in the normal course of business is exempt from the PRA as defined in 5 CFR 1320.3(b)(2).

§ **164.310 Physical safeguards.**

This section requires that a covered entity implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).

We believe that 15,500 entities will have to repair or modify physical components, most of which will need to be done in the first year of implementation. In the following years, we estimate that 500 entities will need to make repairs or modifications. We estimate that it will take 10 minutes to document each repair or modification for a burden of 2,583 hours the first year and 83 hours annually subsequently.

This section requires that a covered entity create a retrievable, exact copy of electronic protected health information, where needed, before movement of equipment.

We believe that the burden associated with this requirement is not subject to the PRA. It is good business practice for entities to backup their data files, and as such is usual and customary among the entities subject to them. A burden associated with a requirement conducted in the normal course of business is exempt from the PRA as defined in 5 CFR 1320.3(b)(2).

§ 164.314 Organizational requirements.

This section requires that a covered entity report to the Secretary problems with a business associate's pattern

of an activity or practice of the business associate that constitute a material breach or violation of the business associate's obligation under the contract or other arrangement if it is not feasible to terminate the contract or arrangement.

We believe that 10 entities will need to comply with this reporting requirement and that it will take them 60 minutes to comply with this requirement for an annual burden of 10 hours.

This section also requires that a covered entity may, if a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in § 160.103 of this subchapter to a covered entity, permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained.

We believe that this situation will affect 20 entities and that it will take 60 minutes to document attempts to obtain assurances and the reasons they cannot be obtained for an annual burden of 20 hours.

This section further requires that business associate contracts or other arrangements and group health plans must require the business entity and plan sponsor, respectively, to report to the covered entity any security incident of which it becomes aware.

We believe that the burden associated with this requirement is not subject to the PRA. It is good business practice for entities to document their agreements via written contracts, and as such is usual and customary among the entities subject to them. A burden associated with a requirement conducted in the normal course of business is exempt from the PRA as defined in 5 CFR 1320.3(b)(2).

§ 164.316 Policies and procedures and documentation requirements.

Paragraph (b)(1), Standard: Documentation, of this section requires a covered entity to--

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity, assessment, or designation is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, assessment, or designation.

We estimate that it will take the 4,000,000 entities covered by this final rule 16 hours to document their polices and procedures, for a total one-time burden of 64,000,000 hours.

The total annual burden of the information collection requirements contained in this final rule is 64,539,264 hours. These information collection requirements will be submitted to OMB for review under the PRA an will not become effective until approved by OMB.

If you comment on these information collection and recordkeeping requirements, please mail copies directly to the following:

Centers for Medicare and Medicaid Services,

Office of Strategic Operations and Regulatory Affairs

Regulations Development and Issuances Group,

Attn: Reports Clearance Officer,

7500 Security Boulevard,

Baltimore, MD 21244-1850,

Attn: Julie Brown, CMS-0049-F; and

Office of Information and Regulatory Affairs,

Office of Management and Budget,

Room 10235, New Executive Office Building,

Washington, DC 20503,

Attn: Brenda Aguilar, CMS Desk Officer.

IV. Regulatory Impact Analysis

A. Overall Impact

We have examined the impacts of this rule as required by Executive Order 12866 (September 1993, Regulatory Planning and Review), the Regulatory Flexibility Act (RFA) (September 16, 1980, Pub. L. 96-354), section 1102(b) of the Social Security Act, the Unfunded Mandates Reform Act of 1995 (Pub. L. 104-4), and Executive Order 13132.

Executive Order 12866 (as amended by Executive Order 13258, which merely reassigns responsibility of duties) directs agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). A regulatory impact analysis (RIA) must be prepared for major rules with economically significant

effects ($100 million or more in any 1 year). Although we cannot determine the specific economic impact of the standards in this final rule (and individually each standard may not have a significant impact), the overall impact analysis makes clear that, collectively, all the standards will have a significant impact of over $100 million on the economy. Because this rule affects over 2 million entities, a requirement as low as $50 per entity would render this rule economically significant. This rule requires each of these entities to engage in, for example, at least some risk assessment activity; thus, this rule is almost certainly economically significant even though we do not have an estimate of the marginal impact of the additional security standards. However, the standards adopted in this rule are considerably more flexible than those anticipated in the overall impact analysis. Therefore, their implementation costs should be lower than those assumed in the impact analysis.

The RFA requires agencies to analyze options for regulatory relief of small businesses. For purposes of the RFA, small entities include small businesses, nonprofit organizations, and government agencies. Most hospitals and most other providers and suppliers are small entities,

either by nonprofit status or by having revenues of $6 million to $29 million in any 1 year. While each standard may not have a significant impact on a substantial number of small entities, the combined effects of all the standards are likely to have a significant effect on a substantial number of small entities. Although we have certified this rule as having a significant impact, we have previously discussed the impact of small entities in the RFA published as part of the August 17, 2000 final regulation for the Standards for Electronic Transactions (65 FR 50312), on pages 50359 through 50360. That analysis included the impact of the set of HIPAA standards regulations (transactions and code sets, identifiers, and security). Although we discussed the impact on small entities in the previous analysis, we would like to discuss how this final rule has been structured to minimize the impact on small entities, compared to the proposed rule.

The proposed rule mandated 69 implementation features for all entities. A large number of commenters indicated that mandating such a large number would be burdensome for all entities. As a result, we have restructured this final rule to permit greater flexibility. While all standards must be met, we are now only requiring 13 implementation

specifications. The remainder of the implementation specifications is "addressable." For addressable specifications, an entity decides whether each specification is a reasonable and appropriate security measure to apply within its particular security framework. This decision is based on a variety of factors, for example, the entity's risk analysis, what measures are already in place, the particular interest to small entities, and the cost of implementation.

Based on the decision, an entity can--(1) implement the specification if reasonable and appropriate; (2) implement an alternative security measure to accomplish the purposes of the standard; or (3) not implement anything if the specification is not reasonable and appropriate and the standard can still be met.

This approach will provide flexibility for all entities, and especially small entities that would be most concerned about the cost and complexity of the security standards. Small entities can look at the addressable implementation specifications and tailor their compliance based on their risks and capabilities of addressing those risks.

The required risk analysis is also a tool to allow flexibility for entities in meeting the requirements of this final rule. The risk analysis requirement is designed to allow entities to look at their own operations and determine the security risks involved. The degree of response is determined by the risks identified. We assume that smaller entities, who deal with smaller amounts of information would have smaller physical facilities, smaller work forces, and therefore, would assume less risk. The smaller amount of risk involved means that the response to that risk can be developed on a smaller scale than that for larger organizations.

Individuals and States are not included in the definition of a small entity. However, the security standards will affect small entities, such as providers and health plans, and vendors in much the same way as they affect any larger entities. Small providers who conduct electronic transactions and small health plans must meet the provisions of this regulation and implement the security standards. A more detailed analysis of the impact on small entities is part of the impact analysis published on August 17, 2000 (65 FR 50312), which provided the impact for all of the HIPAA standards, except privacy. As we

discussed above, the scalability factor of the standards means that the requirements placed upon small providers and plans would be consistent with the complexity of their operations. Therefore, small providers and plans with appropriate security processes in place would need to do relatively little in order to comply with the standards. Moreover, small plans will have an additional year to come into compliance.

In addition, section 1102(b) of the Act requires us to prepare a regulatory impact analysis if a rule may have a significant impact on the operations of a substantial number of small rural hospitals. This analysis must conform to the provisions of section 604 of the RFA. For purposes of section 1102(b) of the Act, we define a small rural hospital as a hospital that is located outside of a Metropolitan Statistical Area and has fewer than 100 beds. While this rule may have a significant impact on small rural hospitals, the impact should be minimized by the scalability factors of the standards, as discussed above in the impact on all small entities. In addition, we have previously discussed the impact of small entities in the RIA published as part of the August 17, 2000 final regulation for the Standards for Electronic Transactions.

Section 202 of the Unfunded Mandates Reform Act (UMRA) of 1995 also requires that agencies assess anticipated costs and benefits before issuing any rule that may result in expenditure in any 1 year by State, local, or tribal governments, in the aggregate, or by the private sector, of $110 million. We estimate that implementation of all the standards will require the expenditure of more than $110 million by the private sector. Therefore, the rule establishes a Federal private sector mandate and is a significant regulatory action within the meaning of section 202 of UMRA (2 U.S.C. 1532). We have included the statements to address the anticipated effects of these rules under section 202.

These standards also apply to State and local governments in their roles as health plans or health care providers. Because these entities, in their roles as health plans or providers, must implement the requirements in these rules, the rules impose unfunded mandates on them. Further discussion of this issue can be found in the previously published impact analysis for all standards (65 FR 50360 through 50361).

The anticipated benefits and costs of the security standards, and other issues raised in section 202 of the

UMRA, are addressed in the analysis below, and in the combined impact analysis. In addition, as required under section 205 of the UMRA (2 U.S.C. 1535), having considered a reasonable number of alternatives as outlined in the preamble to this rule, HHS has concluded that this final rule is the most cost-effective alternative for implementation of HHS's statutory objective of administrative simplification.

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has Federalism implications. The proposed rule was published before the enactment of Executive Order 13132 of August 4, 1999, Federalism (published in the **Federal Register** on August 10, 1999 (64 FR 43255)), which required meaningful and timely input by State and local officials in the development of rules that have Federalism implications). However, we received and considered comments on the proposed rule from State agencies and from entities who conduct transactions with State agencies. Several of the comments referred to the costs that will result from

implementation of the HIPAA standards. As we stated in the impact analysis, we are unable to estimate the cost of implementing security features as implementation needs will vary dependent upon a risk assessment and upon what is already in place. However, the previously referenced impact analysis in the August 17, 2000 final rule (65 FR 50312) showed that Administrative Simplification costs will be offset by future savings.

In complying with the requirements of part C of title XI, the Secretary established interdepartmental implementation teams who consulted with appropriate State and Federal agencies and private organizations. These external groups consisted of the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Standards and Security, the Workgroup for Electronic Data Interchange (WEDI), the National Uniform Claim Committee (NUCC), the National Uniform Billing Committee (NUBC), and the American Dental Association (ADA). The teams also received comments on the proposed regulation from a variety of organizations, including State Medicaid agencies and other Federal agencies.

B. Anticipated Effects

The analysis in the August 2000, Transaction Rule included the expected costs and benefits of the administrative simplification regulations related to electronic systems for 10 years. Although only the electronic transaction standards were promulgated in the transaction rule, HHS expected affected parties to make systems compliance investments collectively because the regulations are so integrated. Moreover, the data available to us were also based on the collective requirements of this regulation. It is not feasible to identify the incremental technological and computer costs for each regulation. Although HHS is issuing rules under HIPAA sequentially, affected entities and vendors are bundling services, that is, they have been anticipating the various needs and are designing relatively comprehensive systems as they develop hardware and software. For example, a vendor developing a system for electronic billing would also anticipate and include security features, even in the absence of any regulation. Moreover, a draft of the security rule was first published in 1998. Even though the final is different (and less burdensome), vendors had a reasonable indication of the direction policy

would go. Thus, in preparing the electronic transaction rule, we recognized and included costs that might theoretically be associated with security or other HIPPA rules. Hence, some of the "costs" of security have already been accounted for in the Standards for Electronic Transactions cost estimate (45 CFR parts 160 and 162), which was published in the **Federal Register** on August 17, 2000 (65 FR 50312).

This analysis showed that the combined impact of the Administrative Simplification standards is expected to save the industry $29.9 billion over 10 years. We are including in each subsequent rule an impact analysis that is specific to the standard or standards in that rule, but the impact analysis will assess only the incremental cost of implementing a given standard over another. Thus, the following discussion contains the impact analysis for the marginal costs of the security standards in this final rule.

The following describes the specific impacts that relate to the security standards. The security of electronic protected health information is, and has been for some time, a basic business requirement that health care entities ignore at their peril. Instances of

"hacking" and other security violations may be widely publicized, and can seriously damage an institution's community standing. Appropriate security protections are crucial for encouraging the growth and use of electronic data interchange. The synergistic effect of the employment of the security standards will enhance all aspects of HIPAA's Administrative Simplification requirements. In addition, it is important to recognize that security is not a one-time project, but rather an on-going, dynamic process.

C. Changes from the 1998 Impact Analysis

The overall impact analysis for Administrative Simplification was first published on May 7, 1998 (63 FR 25320) in the proposed rule for the National Provider Identifier standard (45 CFR part 142), the first of the proposed Administrative Simplification rules. That impact analysis was based on the industry situation at that time, used statistics which were current at that time, and assumed that all of the HIPAA standards would be implemented at roughly the same time, which would permit software changes to be made less expensively. While the original impact analysis represented our best information at that time, we realize that the state of the industry,

and of security technology, has changed since 1998. We discuss several of those changes and how they affect the impact of this regulation.

1. Changes in Technology

The state of technology for health care security has changed since 1998. New technologies to protect information have been developed over the past several years. As a result, HHS has consulted with the Gartner Group, a leading technology assessment organization, regarding what impact these changes in the industry might have on the expected impact of this regulation.

The Gartner analysis indicated that the cost of meeting the requirements of a reasonable interpretation of the security rule in 2002 is probably less than 10 percent higher in 2002 than it was in 1998. This increase is mainly driven by more active threats and increased personnel costs offsetting decreases in technology costs over the past 4 years. However, spending by companies who have anticipated the security rule or who have independently made business decisions to implement security policies and procedures as good business practice(s) has already occurred, and probably will cancel out the increased costs of implementation. Therefore, Gartner expects the cost of

complying with the HIPAA security standards to be about the same now as it was in 1998.

2. Synchronizing Standards

The timelines for the implementation of the initial HIPAA standards (transactions, identifiers, and security) are no longer closely synchronized. However, we do not believe that this lack of synchronization will have a significant impact on the cost of implementing security. The analysis provided by the Gartner group indicated that implementing security standards is being viewed by entities as a separate task from implementing the transaction standards, and that this is not having a significant impact on costs. As with other HIPAA standards, most current entities will have a 2-year implementation period before compliance with the standards is required. Covered entities will develop their own implementation schedules, and may phase in various security measures over that time period.

3. Relationship to Privacy Standards

The publication of the final Privacy Rules (45 CFR parts 160 and 164) on December 28, 2000 in the **Federal Register** (65 FR 82462) and on August 14, 2002

(67 FR 53182) has affected the impact of this regulation significantly. Covered entities must implement the privacy standards by April 14, 2003, (April 14, 2004 for small health plans). The implementation of privacy standards reduces the cost of implementing the security standards in two significant areas.

First, we have made substantial efforts to ensure that the many requirements in the security standards parallel those for privacy, and can easily be satisfied using the solutions for privacy. Administrative requirements like the need for written policies, responsible officers, and business associate agreements that are already required by the Privacy Rule can also serve to meet the security standards without significant additional cost. The analysis of data flows and data uses that covered entities are doing so as to comply with the Privacy Rule should also serve as the starting point for parallel analysis required by this final rule.

Second, it is likely that covered entities will meet a number of the requirements in the security standards through the implementation of the privacy requirements. For example, in order to comply with the Privacy Rule requirements to make reasonable efforts to limit the access

of members of the work force to specified categories of protected health information, covered entities may implement some of the administrative, physical, and technical safeguards that the entity's risk analysis and assessment would require under the Security Rule. E-mail authentication procedures put into place for privacy protection may also meet the security standards, thereby eliminating the need for additional investments to meet these standards. As a result, covered entities that have moved forward in implementing the privacy standards are also implementing security measures at the same time. Since the proposed security standards proposed rule represents the most authoritative guidance now available on the nature of these standards, some entities have been using them to develop their security measures. Those entities should face minimal incremental costs in implementing the final version of these standards.

We are unable to quantify these overlaps, but we believe they may reduce the cost of implementing these security standards. The analysis provided to the HHS by the Gartner Group also stated that compliance with the Privacy Rule will have a moderate effect on the cost of compliance with the Security Rule, reducing it slightly.

4. Sensitivity to Security Concerns as a Result of September 11, 2001

In our discussions with the Gartner Group, they indicated that they saw little evidence of increased security awareness in health care organizations as a result of the events of September 11, 2001. However, a survey conducted by Phoenix Health Systems in the winter of 2002 showed that 65 percent of the respondents to the survey (hospitals, payers, vendors, and clearinghouses) have moderately to greatly increased their attention on overall security. If these organizations have already made investments in security that meet some of the requirements of this rule, it will reduce their added costs of compliance. However, HHS can make no clear statement of the impact of this attention.

D. Guiding Principles for Standard Selection

The implementation teams charged with designating standards under the statute have defined, with significant input from the health care industry, a set of common criteria for evaluating potential standards. These criteria are based on direct specifications in the HIPAA, the purpose of the law, and principles that support the regulatory philosophy set forth in the E.O. 12866 of

September 30, 1993, and the Paperwork Reduction Act of 1995. In order to be designated as such, a standard should do the following:

- Improve the efficiency and effectiveness of the health care system by leading to cost reductions for or improvements in benefits from electronic health care transactions. This principle supports the regulatory goals of cost-effectiveness and avoidance of burden.

- Meet the needs of the health data standards user community, particularly health care providers, health plans, and health care clearinghouses. This principle This principle supports the regulatory goal of cost-effectiveness.

- Be consistent and uniform with the other HIPAA standards (that is, their data element definitions and codes, and their privacy and security requirements) and, secondarily, with other private and public sector health data standards. This principle supports the regulatory goals of consistency and avoidance of incompatibility, and it establishes a performance objective for the standard.

- Have low additional development and implementation costs relative to the benefits of using the standard. This

principle supports the regulatory goals of cost-effectiveness and avoidance of burden.

- Be supported by an ANSI-accredited standards developing organization or other private or public organization that would ensure continuity and efficient updating of the standard over time. This principle supports the regulatory goal of predictability.

- Have timely development, testing, implementation, and updating procedures to achieve administrative simplification benefits faster. This principle establishes a performance objective for the standard.

- Be technologically independent of the computer platforms and transmission protocols used in health transactions, except when they are explicitly part of the standard. This principle establishes a performance objective for the standard and supports the regulatory goal of flexibility.

- Be precise and unambiguous but as simple as possible. This principle supports the regulatory goals of predictability and simplicity.

- Keep data collection and paperwork burdens on users

as low as is feasible. This principle supports the regulatory goals of cost-effectiveness and avoidance of duplication and burden.

- Incorporate flexibility to adapt more easily to changes in the health care infrastructure (for example, new services, organizations, and provider types) and information technology. This principle supports the regulatory goals of flexibility and encouragement of innovation.

We assessed a wide variety of security standards and guidelines against the principles listed above, with the overall goal of achieving the maximum benefit for the least cost. As we stated in the proposed rule, we found that no single standard for security exists that encompasses all the requirements that were listed in the law. However, we believe that the standards we are adopting in this final rule collectively accomplish these goals.

E. Affected Entities

1. Health Care Providers

Covered health care providers may incur implementation costs for establishing or updating their security systems. The majority of costs to implement the security standard (purchase and installation of appropriate computer hardware

and software, and physical safeguards) would generally be incurred in the initial implementation period for the specific requirements of the security standard. Health care providers that do not conduct electronic transactions for which standards have been adopted are not affected by these regulations.

2. Health Plans

All health plans, as the term is defined in regulation at 45 CFR 160.103, must comply with these security standards. In addition, health plans that engage in electronic health care transactions may have to modify their systems to meet the security standards. Health plans that maintain electronic health information may also have to modify their systems to meet the security standards. This conversion would have a one-time cost impact on Federal, State, and private plans alike.

We recognize that this conversion process has the potential to cause business disruption of some health plans. However, health plans would be able to schedule their implementation of the security standards and other standards in a way that best fits their needs, as long as they meet the deadlines specified in the HIPAA law and regulations. Moreover, small plans (many of which are

employer-sponsored) will have an additional year in which to achieve compliance. Small health plans are defined at 45 CFR 160.103 as health plans with annual receipts of $5 million or less.

3. Clearinghouses

All health care clearinghouses must meet the requirements of this regulation. Health care clearinghouses would face effects similar to those experienced by health care providers and health plans. However, because clearinghouses represent one way in which providers and plans can achieve compliance, the clearinghouses' costs of complying with these standards would probably be passed along to those entities, to be shared over the entire customer base.

4. System Vendors

Systems vendors that provide computer software applications to health care providers and other billers of health care services would likely be affected. These vendors would have to develop software solutions that would allow health plans, providers, and other users of electronic transactions to protect these transactions and the information in their databases from unauthorized access

to their systems. Their costs would also probably be passed along to their customer bases.

F. Factors in Establishing the Security Standard

1. General Effect

In assessing the impact of these standards, it is first necessary to focus on the general nature of the standards, their scalability, and the fact that they are not dependent upon specific technologies. These factors will make it possible for covered entities to implement them with the least possible impact on resources. Because there is no national security standard in widespread use throughout the industry, adopting any of the candidate standards would require most health care providers, health plans, and health care clearinghouses to at least conduct an assessment of how their current security measures conform to the new standards. However, we assume that most, if not all, covered entities already have at least some rudimentary security measures in place. Covered entities that identify gaps in their current measures would need to establish or revise their security precautions.

It is also important to note that the standards specify what goals are to be achieved, but give the covered entity some flexibility to determine how to meet those

goals. This is different from the transaction standards, where all covered entities must use the exact same implementation guide. With respect to security, covered entities will be able to blend security processes now in place with new processes. This should significantly reduce compliance costs.

Based on our analysis and comments received, the security standards adopted in this rule do not impose a greater burden on the industry than the options we did not select, and they present significant advantages in terms of universality and flexibility.

We understand that some large health plans, health care providers, and health care clearinghouses that currently exchange health information among trading partners may already have security systems and procedures in place to protect the information from unauthorized access. These entities may not incur significant costs to meet the security standards. Large entities that have sophisticated security systems in place may only need minor revisions or updates to their systems to meet the security standards, or indeed, may not need to make any changes in their systems.

While small providers are not likely to have implemented sophisticated security measures, they are also not as likely to need them as larger covered entities. The scalability principle allows providers to adopt measures that are appropriate to their own circumstances.

2. Complexity of Conversion

The complexity of the conversion to the security standards could be significantly affected by the volume of transactions that covered entities transmit and process electronically and the desire to transmit directly or to use the services of a Value Added Network (VAN) or a clearinghouse. If a VAN or clearinghouse is used, some of the conversion activities would be carried out by that organization, rather than by the covered entity. This would simplify conversion for the covered entity, but makes the covered entity dependent on the success of its business associate. The architecture, and specific technology limitations of existing systems could also affect the complexity of the conversion (for example, certain practice management software that does not contain password protection will require a greater conversion effort than software that has a password protection option already built into it).

3. Cost of Conversion

Virtually all providers, health plans, and clearinghouses that transmit or store data electronically have already implemented some security measures and will need to assess existing security, identify areas of risk, and implement additional measures in order to come into compliance with the standards adopted in this rule. We cannot estimate the per-entity cost of implementation because there is no information available regarding the extent to which providers', plans', and clearinghouses' current security practices are deficient. Moreover, some security solutions are almost cost-free to implement (for example, reminding employees not to post passwords on their monitors), while others are not.

Affected entities will have many choices regarding how they will implement security. Some may choose to assess security using in-house staff, while others will use consultants. Practice management software vendors may also provide security consultation services to their customers. Entities may also choose to implement security measures that require hardware and/or software purchases at the time they do routine equipment upgrades.

The security standards we adopt in this rule were developed with considerable input from the health care industry, including providers, health plans, clearinghouses, vendors, and standards organizations. Industry members strongly advocated the flexible approach we adopt in this rule, which permits each affected entity to develop cost-effective security measures appropriate to their particular needs. We believe that this approach will yield the lowest implementation cost to industry while ensuring that electronic protected health information is safeguarded.

All of the nation's health plans (over 2 million) and providers (over 600,000) will need to conduct some level of gap analysis to assess current procedures against the standards. However, we cannot estimate the number of covered entities that would have to implement additional security systems and procedures to meet the adopted standards. Also, we are not able to estimate the number of providers that do not conduct electronic transactions today but may choose to do so at some future time (these would be entities that send and receive paper transactions and maintain paper records and thus would not be affected). We believe that the security standards represent the minimum

necessary for adequate protection of health information in an electronic format and as such should be implemented by all covered entities. As discussed earlier in this preamble, the security requirements are both scalable and technically flexible; and while the law requires each health plan that is not a small plan to comply with the security and electronic signature requirements no later than 24 months after the effective date of the final rule, small plans will be allowed an additional 12 months to comply.

Since we are unable to estimate the number of entities that may need to make changes to meet the security standards, we are also unable to estimate the cost for those entities. However, we believe that the cost of establishing security systems and procedures is a portion of the costs associated with converting to the administrative simplification standards that are required under HIPAA, which are estimated in the previously referenced impact analysis.

This discussion on conversion costs relates only to health plans, health care providers, and health care clearinghouses that are required to implement the security standards. The cost of implementing security systems and

procedures for entities that do not transmit, receive, or maintain health information electronically is not a cost imposed by the rule, and thus, is not included in our estimates.

G. Alternatives Considered

In developing this final rule, the Department considered some alternatives. One alternative was to not issue a final rule. However, this would not meet the Department's obligations under the HIPAA statute. It would also leave the health industry without a set of standards for protecting the security of health information. The vast majority of commenters supported our efforts in developing a set of standards. Thus, we concluded that not publishing a final rule was not in the best interests of the industry and not in the best interests of persons whose medical information will be protected by these measures.

A second alternative was to publish the final rule basically unchanged from the proposed rule. Although most commenters supported the approach of the proposed rule, there were significant objections to the number of required specifications, concerns about the scope of certain requirements, duplication and ambiguity of some requirements, and the overall complexity of the approach.

Based on those comments, it was clear that revisions had to be made. In addition, the proposed rule was developed before the Privacy Rule requirements were developed. Thus, it did not allow for any alignment of requirements between the Privacy and Security standards.

As a result, the Department determined that an approach that modified the proposed rule and aligned the requirements with the Privacy standards was the preferred alternative.

V. Federalism

Executive Order 13132 of August 4, 1999, Federalism, published in the **Federal Register** on August 10, 1999 (64 FR 43255), requires us to ensure meaningful and timely input by State and local officials in the development of rules that have Federalism implications. Although the proposed rule for security standards was published before the enactment of this Executive Order, the Department consulted with State and local officials as part of an outreach program in the process of developing the proposed regulation. The Department received comments on the proposed rule from State agencies and from entities that conduct transactions with State agencies. Many of these comments were concerned with the burden that the proposed

security standards would place on their organizations. In response to those comments, we have modified the security standards to make them more flexible and less burdensome.

In complying with the requirements of part C of Title XI, the Secretary established an interdepartmental team who consulted with appropriate State and Federal agencies and private organizations. These external groups included the NCVHS Workgroup on Standards and Security, the Workgroup for Electronic Data Interchange, the National Uniform Claim Committee, and the National Uniform Billing Committee. Most of these groups have State officials as members. We also received comments on the proposed regulation from these organizations.

In accordance with the provisions of Executive Order 12866, this rule has been reviewed by the Office of Management and Budget.

List of Subjects

45 CFR Part 160

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

45 CFR Part 162

Administrative practice and procedure, Health facilities, Health insurance, Hospitals, Medicaid, Medicare, report and recordkeeping requirement.

45 CFR Part 164

Administrative practice and procedure, Health facilities, Health insurance, Hospitals, Medicaid, Medicare, Electronic Information System, Security, Report and recordkeeping requirement.

For the reasons set forth in the preamble, the Department of Health and Human Services amends title 45, subtitle A, subchapter C, parts 160, 162, and 164 as set forth below:

PART 160--GENERAL ADMINISTRATIVE REQUIREMENTS

1. The authority citation for part 160 continues to read as follows:

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

2. In § 160.103, the definitions of "disclosure", "electronic media", "electronic protected health information," "individual," "organized health care arrangement", "protected health information," and "use" are added in alphabetical order to read as follows:

§ 160.103 Definitions.

* * * * *

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

* * * * *

Electronic media means:

(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Electronic protected health information means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section.

* * * * *

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

* * * * *

Organized health care arrangement means:

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

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

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

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

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

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

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

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

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

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to

individuals who are or have been participants or beneficiaries in any of such group health plans.

Protected health information means individually identifiable health information:

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

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

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

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

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

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

(iii) Employment records held by a covered entity in its role as employer.

* * * * *

Use means, with respect to individually identifiable health information, the sharing, employment, application,

utilization, examination, or analysis of such information within an entity that maintains such information.

* * * * *

PART 162--ADMINISTRATIVE REQUIREMENTS

1. The authority citation for part 162 is revised to read as follows:

Authority: Secs. 1171 through 1179 of the Social Security Act (42 U.S.C. 1320d-1320d-8), as added by sec. 262 of Pub. L. 104-191, 110 Stat. 2021-2031, and sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)).

§ 162.103 [Amended]

2. In § 162.103, the definition of "electronic media" is removed.

PART 164--SECURITY AND PRIVACY

1. The authority citation for part 164 is revised to read as follows:

Authority: Secs. 1171 through 1179 of the Social Security Act (42 U.S.C. 1320d-1320d-8), as added by sec. 262 of Pub. L. 104-191, 110 Stat. 2021-2031, and 42 U.S.C. 1320d-2 and 1320d-4, sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)).

2. A new § 164.103 is added to read as follows:

§ 164.103 Definitions.

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

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

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

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

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with § 164.105(a)(2)(iii)(C).

Hybrid entity means a single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with paragraph § 164.105(a)(2)(iii)(C).

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

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

3. Section 164.104 is revised to read as follows:

§ 164.104 Applicability.

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

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health

information in electronic form in connection with a transaction covered by this subchapter.

(b) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, or other than as a business associate of a covered entity, the clearinghouse must comply with § 164.105 relating to organizational requirements for covered entities, including the designation of health care components of a covered entity.

4. A new § 164.105 is added to read as follows:

§ 164.105 Organizational requirements.

(a)(1) Standard: Health care component. If a covered entity is a hybrid entity, the requirements of subparts C and E of this part, other than the requirements of this section, § 164.314, and § 164.504, apply only to the health care component(s) of the entity, as specified in this section.

(2) Implementation specifications:

(i) Application of other provisions. In applying a provision of subparts C and E of this part, other than the requirements of this section, § 164.314, and § 164.504, to a hybrid entity:

(A) A reference in such provision to a "covered

entity" refers to a health care component of the covered entity;

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

(C) A reference in such provision to "protected health information" refers to protected health information that is created or received by or on behalf of the health care component of the covered entity; and

(D) A reference in such provision to "electronic protected health information" refers to electronic protected health information that is created, received, maintained, or transmitted by or on behalf of the health care component of the covered entity.

(ii) Safeguard requirements. The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this section and subparts C and E of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

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

(B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities;

(C) A component that is described by paragraph (a)(2)(iii)(C)(2) of this section does not use or disclose protected health information that it creates or receives from or on behalf of the health care component in a way prohibited by subpart E of this part;

(D) A component that is described by paragraph (a)(2)(iii)(C)(2) of this section that creates, receives, maintains, or transmits electronic protected health information on behalf of the health care component is in compliance with subpart C of this part; and

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

(iii) Responsibilities of the covered entity. A covered entity that is a hybrid entity has the following responsibilities:

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

(B) The covered entity is responsible for complying with § 164.316(a) and § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this section and subparts C and E of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section.

(C) The covered entity is responsible for designating the components that are part of one or more health care

components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates a health care component or components, it must include any component that would meet the definition of covered entity if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs:

(1) Covered functions; or

(2) Activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.

(b)(1) Standard: Affiliated covered entities. Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of subparts C and E of this part.

(2) Implementation specifications:

(i) Requirements for designation of an affiliated covered entity.

(A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for

purposes of subparts C and E of this part, if all of the covered entities designated are under common ownership or control.

(B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section.

(ii) Safeguard requirements. An affiliated covered entity must ensure that:

(A) The affiliated covered entity's creation, receipt, maintenance, or transmission of electronic protected health information complies with the applicable requirements of subpart C of this part;

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

(C) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with § 164.308(a)(4)(ii)(A) and § 164.504(g), as applicable.

(c)(1) Standard: Documentation. A covered entity must maintain a written or electronic record of a

designation as required by paragraphs (a) or (b) of this section.

(2) Implementation specification: Retention period. A covered entity must retain the documentation as required by paragraph (c)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

5. A new subpart C is added to part 164 to read as follows:

Subpart C--Security Standards for the Protection of Electronic Protected Health Information

Sec.

Appendix A to Subpart C of Part 164-Security Standards: Matrix

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

§ 164.302 Applicability.

A covered entity must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information.

§ 164.304 Definitions.

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

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subpart E of this part.)

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Authentication means the corroboration that a person is the one claimed.

Availability means the property that data or information is accessible and useable upon demand by an authorized person.

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility means the physical premises and the interior and exterior of a building(s).

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

Malicious software means software, for example, a virus, designed to damage or disrupt a system.

Password means confidential authentication information composed of a string of characters.

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Security or Security measures encompass all of the administrative, physical, and technical safeguards in an information system.

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

User means a person or entity with authorized access.

Workstation means an electronic computing device, for

example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

§ 164.306 Security standards: General rules.

(a) General requirements. Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

(b) Flexibility of approach.

(1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity.

(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

(c) Standards. A covered entity must comply with the standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314, and § 164.316 with respect to all electronic protected health information.

(d) Implementation specifications.

In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity must implement the implementation specifications.

(3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity must--

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and

(ii) As applicable to the entity--

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate--

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

(e) Maintenance. Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at § 164.316.

§ 164.308 Administrative safeguards.

(a) A covered entity must, in accordance with § 164.306:

(1)(i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) Implementation specifications:

(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

(3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) Implementation specifications:

(A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic

protected health information or in locations where it might be accessed.

(B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) Implementation specifications:

(A) Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

(5)(i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).

(ii) Implementation specifications. Implement:

(A) Security reminders (Addressable). Periodic security updates.

(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

(C) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.

(6)(i) Standard: Security incident procedures. Implement policies and procedures to address security incidents.

(ii) Implementation specification: Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

(7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) Implementation specifications:

(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

(b)(1) Standard: Business associate contracts and other arrangements. A covered entity, in accordance with

§ 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.

(2) This standard does not apply with respect to--

(i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual.

(ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met; or

(iii) The transmission of electronic protected health information from or to other agencies providing the services at § 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met.

(3) A covered entity that violates the satisfactory assurances it provided as a business associate of another

covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

(4) Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

§ 164.310 Physical safeguards.

A covered entity must, in accordance with § 164.306:

(a)(1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) Implementation specifications:

(i) Contingency operations (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) Access control and validation procedures (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) Standard: Workstation use. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

(c) Standard: Workstation security. Implement physical safeguards for all workstations that access

electronic protected health information, to restrict access to authorized users.

(d)(1) Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) Implementation specifications:

(i) Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

(ii) Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

(iii) Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

(iv) Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

§ 164.312 Technical safeguards.

A covered entity must, in accordance with § 164.306:

(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) Implementation specifications:

(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.

(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) Implementation specifications:

(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

§ 164.314 Organizational requirements.

(a)(1) Standard: Business associate contracts or other arrangements.

(i) The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.

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

or end the violation, as applicable, and, if such steps were unsuccessful.

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

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

(2) Implementation specifications (Required).

(i) Business associate contracts. The contract between a covered entity and a business associate must provide that the business associate will--

(A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

(B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;

(C) Report to the covered entity any security incident of which it becomes aware;

(D) Authorize termination of the contract by the covered entity, if the covered entity determines that the

business associate has violated a material term of the contract.

(ii) Other arrangements.

(A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if--

(1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or

(2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section.

(B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph

(a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained.

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

(b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

(2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to--

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

§ 164.316 Policies and procedures and documentation requirements.

A covered entity must, in accordance with § 164.306:

(a) Standard: Policies and procedures. Implement reasonable and appropriate policies and procedures to

comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

(b)(1) Standard: Documentation.

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

(2) Implementation specifications:

(i) Time limit (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(ii) Availability (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(iii) Updates (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

§ 164.318 Compliance dates for the initial implementation of the security standards.

(a) Health plan.

(1) A health plan that is not a small health plan must comply with the applicable requirements of this subpart no later than **[OFR: insert date 26 months after the date of publication in the Federal Register].**

(2) A small health plan must comply with the applicable requirements of this subpart no later than **[OFR: insert date 38 months after the date of publication in the Federal Register].**

(b) Health care clearinghouse. A health care clearinghouse must comply with the applicable requirements of this subpart no later than **[OFR: insert date 26 months after the date of publication in the Federal Register].**

(c) Health care provider. A covered health care provider must comply with the applicable requirements of this subpart no later than **[OFR: insert date 26 months after the date of publication in the Federal Register].**

Appendix A to Subpart C of Part 164

Security Standards: Matrix

ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedure	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement	(R)

PHYSICAL SAFEGUARDS

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		(R)
Workstation Security	164.310(c)		(R)
Device and Media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

TECHNICAL SAFEGUARDS (see § 164.312)

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312(b)		(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312(d)		(R)
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

§ 164.500 [Amended]

6. In 164.500(b)(1)(iv), remove the words "including the designation of health care components of a covered entity".

§ 165.501 [Amended]

7. In § 164.501, the definitions of the following terms are removed: Covered functions, Disclosure, Individual, Organized health care arrangement, Plan sponsor Protected health information, Required by law, and Use.

§ 164.504 [Amended]

8. In §164.504, the following changes are made:

a. The definitions of the following terms are removed: Common control, Common ownership, Health care component, and Hybrid entity.

b. Paragraphs (b) through (d) are removed and reserved.

Dated: _____

_____

Tommy G. Thompson,

Secretary.

Billing Code 4120-01-P