DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Part 142

[HCFA–0049–P]

RIN 0938–AI57

Security and Electronic Signature Standards

AGENCY: Health Care Financing Administration (HCFA), HHS.

ACTION: Proposed rule.

SUMMARY: This rule proposes standards for the security of individual health information and electronic signature use by health plans, health care clearinghouses, and health care providers. The health plans, health care clearinghouses, and health care providers would use the security standards to develop and maintain the security of all electronic individual health information. The electronic signature standard is applicable only with respect to use with the specific transactions defined in the Health Insurance Portability and Accountability Act of 1996, and when it has been determined that an electronic signature must be used.

The use of these standards would 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. This rule would implement some of the requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996.

DATES: Comments will be considered if we receive them at the appropriate address, as provided below, no later than 5 p.m. on October 13, 1998.

ADDRESSES: Mail written comments (1 original and 3 copies) to the following address: Health Care Financing Administration, Department of Health and Human Services, Attention: HCFA–0049–P, P.O. Box 26585, Baltimore, MD 21207–0519.

If you prefer, you may deliver your written comments (1 original and 3 copies) to one of the following addresses:

Room 309–G, Hubert H. Humphrey Building, 200 Independence Avenue, SW., Washington, DC 20201, or

Room C5–09–26, 7500 Security Boulevard, Baltimore, MD 21244–1850.

Comments may also be submitted electronically to the following e-mail address: security@osaspe.dhhs.gov. For e-mail comment procedures, see the beginning of **SUPPLEMENTARY INFORMATION.** For further information on ordering copies of the **Federal Register** containing this document and on electronic access, see the beginning of **SUPPLEMENTARY INFORMATION.**

FOR FURTHER INFORMATION CONTACT: John Parmigiani, (410) 786–2976.

SUPPLEMENTARY INFORMATION:

E-Mail, Comments, Procedures, Availability of Copies, and Electronic Access

E-mail comments should include the full name, postal address, and affiliation (if applicable) of the sender and must be submitted to the referenced address to be considered. All comments should be incorporated in the e-mail message because we may not be able to access attachments.

Because of staffing and resource limitations, we cannot accept comments by facsimile (FAX) transmission. In commenting, please refer to file code HCFA–0049–P and the specific section or sections of the proposed rule. Both electronic and written comments received by the time and date indicated above will be available for public inspection as they are received, generally beginning approximately 3 weeks after publication of a document, in Room 309–G of the Department's offices at 200 Independence Avenue, SW., Washington, DC, on Monday through Friday of each week from 8:30 a.m. to 5 p.m. (phone: (202) 690–7890). Electronic and legible written comments will also be posted, along with this proposed rule, at the following web site: http://aspe.os.dhhs.gov/admnsimp/.

Copies: 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 $8. 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. Free public access is available on a Wide Area Information Server (WAIS) through the Internet and via asynchronous dial-in. Internet users can access the database by using the World Wide Web, http://www.access.gpo.gov/nara/, by using local WAIS client software, or by telnet to swais.access.gpo.gov, then login as guest (no password required). Dial-in users should use communications software and modem to call (202) 512–1661; type swais, then login as guest (no password required).

I. Background

[Please label written or e-mailed comments about this section with the subject: Background]

In order to administer their programs, the Department of Health and Human Services, other Federal agencies, State Medicaid agencies, private health plans, health care providers, and health care clearinghouses must assure their customers (such as patients, insured, providers, and health care plans) that the confidentiality and privacy of health care information they electronically collect, maintain, use, or transmit is secure. Security of health information is especially important when health information can be directly linked to an individual.

Confidentiality is threatened not only by the risk of improper access to electronically stored information, but also by the risk of interception during electronic transmission of the information.

In addition to the need to ensure electronic health care information is secure and confidential, there is a potential need to associate signature capability with information being electronically stored or transmitted. Today, there are numerous forms of electronic signatures, ranging from biometric devices to digital signature. To satisfy the legal and time-tested characteristics of a written signature, however, an electronic signature must do the following:

- Identify the signatory individual,
- Assure the integrity of a document's content, and
- Provide for nonrepudiation; that is, strong and substantial evidence that will make it difficult for the signer to claim that the electronic representation is not valid. Currently, the only technically mature electronic signature meeting the above criteria is the digital signature. There is no national standard for security or electronic signatures. Of necessity, each health care provider, health care plan, and health care entity

has defined its own security requirements.

A. Legislation

The Congress included provisions to address the need for security and electronic signature standards and other administrative simplification issues in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191, which was enacted on August 21, 1996. Through 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.'' (Public Law 104–191 affects several titles in the United States Code. 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 this part C is to improve the Medicare and Medicaid programs, in particular, and the efficiency and effectiveness of the health care system, in general, by encouraging the development of a health information system through the establishment of standards and requirements to facilitate the electronic maintenance and transmission of certain health information.

Part C of title XI of the Act consists of sections 1171 through 1179. These sections define various terms and impose several requirements on HHS, health plans, health care clearinghouses, and certain health care providers concerning electronic transmission of health information.

The first section, section 1171 of the Act, establishes definitions for purposes of part C of title XI for the following terms: code set, health care clearinghouse, health care provider, health information, health plan, individually identifiable health information, standard, and standard setting organization.

Section 1172 of the Act makes any standard adopted under part C applicable to: (1) Health plans, (2) health care clearinghouses, and (3) health care providers that transmit any health information in electronic form in connection with the transactions referred to in section 1173(a)(1) of the Act. The security standard to be adopted under Part C is not restricted to the transactions referred to in section 1173(a)(1) of the Act, but is applicable to any health information pertaining to an individual that is electronically maintained or transmitted. This section also contains the following requirements concerning standard setting:

- The Secretary may adopt a standard developed, adopted, or modified by a standard setting organization (that is, an organization accredited by the American National Standards Institute (ANSI)) that has consulted with the National Uniform Billing Committee (NUBC), the National Uniform Claim Committee (NUCC), Workgroup for Electronic Data Interchange (WEDI), and the American Dental Association (ADA).
- The Secretary may also adopt a standard other than one established by a standard setting organization, if the different standard will reduce costs for health care providers and health plans, the different standard is promulgated through negotiated rulemaking procedures, and the Secretary consults with each of the above-named groups.
- If no standard has been adopted by any standard setting organization, the Secretary must rely on the recommendations of the National Committee on Vital and Health Statistics (NCVHS) and consult with each of the above-named groups.

In complying with the requirements of part C of title XI, the Secretary must rely on the recommendations of the NCVHS, consult with appropriate State, Federal, and private agencies or organizations, and publish the NCVHS recommendations in the **Federal Register**.

Paragraph (a) of section 1173 of the Act requires that the Secretary adopt standards for financial and administrative transactions, and data elements for those transactions, to enable health information to be exchanged electronically. Standards are required for the following transactions: health claims, health encounter information, health claims attachments, health plan enrollments and disenrollments, health plan eligibility, health care payment and remittance advice, health plan premium payments, first report of injury, health claim status, and referral certification and authorization. In addition, the Secretary is required to adopt standards for any other financial and administrative transactions that are determined to be appropriate by the Secretary.

Paragraph (b) of section 1173 of the Act requires the Secretary to adopt standards for unique health identifiers for all individuals, employers, health plans, and health care providers and requires further that the adopted standards specify for what purposes unique health identifiers may be used.

Paragraphs (c) through (f) of section 1173 of the Act require the Secretary to establish standards for code sets for each data element for each health care transaction listed above, security standards for health care information systems, standards for electronic signatures (established together with the Secretary of Commerce), and standards for the transmission of data elements needed for the coordination of benefits and sequential processing of claims. Compliance with electronic signature standards will be deemed to satisfy both State and Federal requirements for written signatures with respect to the transactions listed in paragraph (a) of section 1173 of the Act.

In section 1174 of the Act, the Secretary is required to establish standards for all of the above transactions, except claims attachments, by February 21, 1998. The standards for claims attachments must be established by February 21, 1999. Generally, after a standard is established, it cannot be changed during the first year after adoption except for changes that are necessary to permit compliance with the standard. Modifications to any of these standards may be made after the first year, but not more frequently than once every 12 months. The Secretary must also ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets and that there are crosswalks from prior versions.

Section 1175 of the Act prohibits health plans from refusing to process or delaying the processing of a transaction that is presented in standard format. The Act's requirements are not limited to health plans; however, each person to whom a standard or implementation specification applies is required to comply with the standard within 24 months (or 36 months for small health plans) of its adoption. A health plan or other entity may, of course, comply voluntarily before the effective date. A person may comply by using a health care clearinghouse to transmit or receive the standard transactions. Compliance with modifications to standards or implementation specifications must be accomplished by a date designated by the Secretary. This date may not be earlier than 180 days from the notice of change.

Section 1176 of the Act establishes a civil monetary penalty for violation of the provisions in part C of title XI of the Act, subject to several limitations. Penalties may not be more than $100 per person per violation and not more than $25,000 per person for violations of a single standard for a calendar year. The procedural provisions in section 1128A of the Act, ''Civil Monetary Penalties,'' are applicable.

Section 1177 of the Act establishes penalties for a knowing misuse of unique health identifiers and individually identifiable health information: (1) A fine of not more than $50,000 and/or imprisonment of not

more than 1 year; (2) if misuse is ''under false pretenses,'' a fine of not more than $100,000 and/or imprisonment of not more than 5 years; and (3) if misuse is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than 10 years. Note that these penalties do not affect any other penalties which may be imposed by other Federal programs, including ERISA.

Under section 1178 of the Act, the provisions of part C of title XI of the Act, as well as any standards established under them, supersede any State law that is contrary to them. However, the Secretary may, for statutorily-specified reasons, waive this provision.

Finally, section 1179 of the Act makes the above provisions inapplicable to financial institutions or anyone acting on behalf of a financial institution when ''authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for a financial institution.''

(Concerning this last provision, the conference report, in its discussion on section 1178, states:

''The conferees do not intend to exclude the activities of financial institutions or their contractors from compliance with the standards adopted under this part if such activities would be subject to this part. However, conferees intend that this part does not apply to use or disclosure of information when an individual utilizes a payment system to make a payment for, or related to, health plan premiums or health care. For example, the exchange of information between participants in a credit card system in connection with processing a credit card payment for health care would not be covered by this part. Similarly sending a checking account statement to an account holder who uses a credit or debit card to pay for health care services, would not be covered by this part. However, this part does apply if a company clears health care claims, the health care claims activities remain subject to the requirements of this part.'') (H.R. Rep. No. 736, 104th Cong., 2nd Sess. 268–269 (1996))

B. Process for Developing National Standards

The Secretary has formulated a five-part strategy for developing and implementing the standards mandated under part C of title XI of the Act:

1. To ensure necessary interagency coordination and required interaction with other Federal departments and the private sector, establish interdepartmental implementation teams to identify and assess potential standards for adoption. The subject matter of the teams includes claims/encounters, identifiers, enrollment/eligibility, systems security and electronic signature, and medical coding classification. Another team addresses cross-cutting issues and coordinates the subject matter teams. The teams consult with external groups such as the NCVHS' Workgroup on Data Standards, WEDI, the ANSI's Healthcare Informatics Standards Board (HISB), the NUCC, the NUBC, and the ADA. The teams are charged with developing regulations and other necessary documents and making recommendations for the various standards to the HHS Data Council through its Committee on Health Data Standards. (The HHS Data Council is the focal point for consideration of data policy issues. It reports directly to the Secretary and advises the Secretary on data standards and privacy issues.)

2. Develop recommendations for standards to be adopted.

3. Publish proposed rules in the **Federal Register** describing the standards. Each proposed rule provides the public with a 60-day comment period.

4. Analyze public comments and publish the final rules in the **Federal Register**.

5. Distribute standards and coordinate preparation and distribution of implementation guides.

This strategy affords many opportunities for involvement of interested and affected parties in standards development and adoption by enabling them to:

- Participate with standards setting organizations.
- Provide written input to the NCVHS.
- Provide written input to the Secretary of HHS.
- Provide testimony at NCVHS'' public meetings.
- Comment on the proposed rules for each of the proposed standards.
- Invite HHS staff to meetings with public and private sector organizations or meet directly with senior HHS staff involved in the implementation process.

The implementation teams charged with reviewing standards for designation as required national standards under the statute have defined, with significant input from the health care industry, a set of principles for guiding choices for the standards to be adopted by the Secretary. These principles are based on direct specifications in HIPAA, the purpose of the law, and generally desirable principles. To be designated as an HIPAA standard, each standard should:

1. 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.

2. Meet the needs of the health data standards user community, particularly health care providers, health plans, and health care clearinghouses.

3. Be consistent and uniform with the other HIPAA standards—their data element definitions and codes and their privacy and security requirements—and, secondarily, with other private and public sector health data standards.

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

5. Be supported by an ANSI-accredited standards developing organization or other private or public organization that will ensure continuity and efficient updating of the standard over time.

6. Have timely development, testing, implementation, and updating procedures to achieve administrative simplification benefits faster.

7. Be technologically independent of the computer platforms and transmission protocols used in electronic health transactions, except when they are explicitly part of the standard.

8. Be precise and unambiguous, but as simple as possible.

9. Keep data collection and paperwork burdens on users as low as is feasible.

10. Incorporate flexibility to adapt more easily to changes in the health care infrastructure (such as new services, organizations, and provider types) and information technology.

A master data dictionary providing for common data definitions across the standards selected for implementation under HIPAA will be developed and maintained. We intend for the data element definitions to be precise, unambiguous, and consistently applied. The transaction-specific reports and general reports from the master data dictionary will be readily available to the public. At a minimum, the information presented will include data element names, definitions, and appropriate references to the transactions where they are used.

This proposed rule would establish the security standard and electronic signature standard for health care information and individually identifiable health care information maintained or transmitted electronically. The remaining standards are grouped, to the extent possible, by subject matter and audience in other regulations. We anticipate publishing

several separate regulation documents to promulgate the remaining standards required under HIPAA.

II. Provisions of this Proposed Rule

[Please label written comments or e-mailed comments about this section with the subject: Introduction/Applicability]

We propose to add a new part to title 45 of the Code of Federal Regulations for health plans, health care providers, and health care clearinghouses in general. The new part would be part 142 of title 45 and would be titled ''Administrative Requirements.'' Subpart A would contain the general provisions for this part, including the general definitions and general requirements for health plans. Subpart C would contain provisions specific to securing health information used in any electronic transmission or stored format.

In this proposed rule, we propose a standard for security of health information. This rule would establish that health plans, health care clearinghouses, and health care providers must have the security standard in place to comply with the statutory requirement that health care information and individually identifiable health care information be protected to ensure privacy and confidentiality when health information is electronically stored, maintained, or transmitted. The Congress mandated a separate standard for electronic signature, therefore, this proposed security standard also addresses the selected standard for electronic signature. The proposed security standard does not require the use of an electronic signature, but specifies the standard for an electronic signature that must be followed if such a signature is used. If an entity elects to use an electronic signature, it must comply with the electronic signature standard.

A. Applicability

With the exception of the security provisions, section 262 of HIPAA applies to any health plan, any health care clearinghouse, and any health care provider that transmits any health information in electronic form in connection with transactions referred to in section 1173(a)(1) of the Act. The security provisions of section 262 of HIPAA apply to any health plan, any health care clearinghouse, and any health care provider that electronically maintains or transmits any health information relating to an individual.

Our proposed rules (at 45 CFR 142.102) would apply to the health plans and health care clearinghouses as well, but we would clarify the statutory language in our regulations for health care providers. With the exception of the security regulation, we would have the regulations apply to any health care provider only when electronically transmitting any of the transactions to which section 1173(a)(1) of the Act refers.

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 compact disc (cd) 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 are all included. Telephone voice response and ''faxback'' (a request for information made via voice using a fax machine and requested information returned via that same machine as a fax) systems would not be included. We solicit comments concerning any adverse impact the above statement concerning voice response or faxback may have upon the security of the health information in the commenter's care.

With the exception of the security regulation, our regulations would apply to health care clearinghouses when transmitting transactions to, and receiving transactions from, a health care provider or health plan that transmits and receives standard transactions (as defined under ''transaction'') and at all times when transmitting to or receiving electronic transactions from another health care clearinghouse. The security regulation would apply to health care clearing houses electronically maintaining or transmitting any health information pertaining to an individual.

Entities that offer on-line interactive transmission must comply with the standards. The Hypertext Markup Language (HTML) interaction between a server and a browser by which the data elements of a transaction are solicited from a user would not have to use the standards (with the exception of the security standard), although the data content must be equal to that required for the standard. Once the data elements are assembled into a transaction by the server, the transmitted transaction would have to comply with the standards.

With the exception of the security portion, the law would apply to each health care provider when transmitting or receiving any of the specified electronic transactions. The security regulation would apply to each health care provider electronically maintaining or transmitting any health information pertaining to an individual.

The law applies to health plans for all transactions. Section 142.104 would contain the following provisions (from section 1175 of the Act):

If a person desires to conduct a transaction (as defined in § 142.103) with a health plan as a standard transaction, the following apply:

(1) The health plan may not refuse to conduct the transaction as a standard transaction.

(2) The health plan may not delay the transaction or otherwise adversely affect, or attempt to adversely affect, the person or the transaction on the basis that the transaction is a standard transaction.

(3) The information transmitted and received in connection with the transaction must be in the form of standard data elements of health information.

As a further requirement, we would provide that a health plan that conducts transactions through an agent assure that the agent meets all the requirements of part 142 that apply to the health plan.

Section 142.105 would state that a person or other entity may meet the transaction requirements of § 142.104 by either—

(1) Transmitting and receiving standard data elements, or

(2) Submitting nonstandard data elements to a health care clearinghouse for processing into standard data elements and transmission by the health care clearinghouse and receiving standard data elements through the clearinghouse.

Health care clearinghouses would be able to accept nonstandard transactions for the sole purpose of translating them into standard transactions for sending customers and would be able to accept standard transactions and translate them into nonstandard formats for receiving customers. We would state in § 142.105 that the transmission of nonstandard transactions, under contract, between a health plan or a health care provider and a health care clearinghouse would not violate the law.

With the exception of the security standard, transmissions within a corporate entity would not be required to comply with the standards. A hospital that is wholly owned by a managed care company would not have to use the transaction standards to pass encounter information back to the home office, but it would have to use the standard claims transaction to submit a claim to another payer. Another example might be transactions within Federal agencies and their contractors and between State agencies within the same State. For example, Medicare enters into contracts with insurance

companies and common working file sites that process Medicare claims using government furnished software. There is constant communication, on a private network, between HCFA Central Office and the Medicare carriers, intermediaries, and common working file sites. This communication may continue in nonstandard mode. However, these contractors would be required to comply with the transaction standards when exchanging any of the transactions covered by HIPAA with an entity outside these ''corporate'' boundaries.

The security standard is applicable to all health care information electronically maintained or used in an electronic transmission, regardless of format (standard transaction or a proprietary format); no distinction is made between internal corporate entity communication or communication external to the corporate entity.

Although there are situations in which the use of the standards is not required (for example, health care providers may continue to submit paper claims and employers are not required to use any of the standard transactions), we stress that a standard may be used voluntarily in any situation in which it is not required.

This proposed regulation would not mandate the use of electronic signatures with any specific transaction at this time. Instead, the regulation proposes that whenever an electronic signature is required for an electronic transaction by law, regulation, or contract, the signature must meet the standard established in the regulation at § 142.310. Use of this standard would satisfy any Federal or State requirement for a signature, either electronic or on paper.

We note that the ANSI X12N standards for individual transactions which have been proposed for adoption as national standards in a separate proposed rule do not require the use of electronic signatures. Standards for additional transactions that the Secretary may propose for adoption in the future, including one for claims attachments, may contain such requirements. We solicit comments on whether electronic signatures should be required for any specific transactions or under specific circumstances and what effect such requirements would have on electronic health care transactions.

We also note that the NCVHS is required by HIPAA to report to the Secretary recommendations and legislative proposals for uniform data standards for patient medical record information and the electronic exchange of such information, with the implication that HHS should rely on such recommendations to adopt such standards or propose the passage of such legislation by the Congress. We solicit comments on whether the standard proposed below for electronic signatures would be appropriate for consideration as part of such standards.

B. Definitions

[Please label written or e-mailed comments about this section with the subject: Definitions]

Section 1171 of the Act defines several terms and our proposed rules would, for the most part, simply restate the law. The terms that we are defining in this proposed rule follow:

1. Code Set

We would define ''code set'' as section 1171(1) of the Act does: ''code set'' means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

2. Health Care Clearinghouse

We would define ''health care clearinghouse'' as section 1171(2) of the Act does, but we are adding a further, clarifying sentence. The statute defines a ''health care clearinghouse'' as a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. We would further explain that such an entity is one that currently receives health care transactions from health care providers or other entities, translates the data from a given format into one acceptable to the intended recipient and forwards the processed transaction to appropriate payers and clearinghouses, as necessary, for further action.

There are currently a number of private clearinghouses that perform this function for health care providers. For purposes of this rule, we would consider billing services, repricing companies, community health management information systems or community health information systems, value-added networks, and switches that perform this function to be health care clearinghouses.

3. Health Care Provider

As defined by section 1171(3) of the Act, a ''health care provider'' is a provider of services as defined in section 1861(u) of the Act, a provider of medical or other health services as defined in section 1861(s) of the Act, and any other person who furnishes health care services or supplies. Our regulations would define ''health care provider'' as the statute does and clarify that the definition of a health care provider is limited to those entities that furnish, or bill and are paid for, health care services in the normal course of business.

For a more detailed discussion of the definition of health care provider, we refer the reader to our proposed rule, HCFA–0045-P, Standard Health Care Provider, 63 FR 25320, published May 7, 1998.

4. Health Information

''Health information,'' as defined in section 1171 of the Act, means any information, whether oral or recorded in any form or medium, that—

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

We propose the same definition for our regulations.

5. Health Plan

We propose that a ''health plan'' be defined essentially as section 1171 of the Act defines it. Section 1171 of the Act cross refers to definitions in section 2791 of the Public Health Service Act (as added by Public Law 104–191, 42 U.S.C. 300gg-91); we would incorporate those definitions as currently stated into our proposed definitions for the convenience of the public. We note that the term ''health plan'' is also defined in other statutes, such as the Employee Retirement Income Security Act of 1974 (ERISA). Our definitions are based on the roles of plans in conducting administrative transactions, and any differences should not be construed to affect other statutes.

For purposes of implementing the provisions of administrative simplification, a ''health plan'' would be an individual or group health plan that provides, or pays the cost of, medical care. This definition includes, but is not limited to, the 13 types of plans listed in the statute. On the other hand, plans such as property and casualty insurance plans and workers compensation plans, which may pay health care costs in the course of administering nonhealth care benefits, are not considered to be health plans in the proposed definition of health plan. Of course, these plans may voluntarily adopt these standards for their own business needs. At some

future time, the Congress may choose to expressly include some or all of these plans in the list of health plans that must comply with the standards.

Health plans often carry out their business functions through agents, such as plan administrators (including third party administrators), entities that are under ''administrative services only'' (ASO) contracts, claims processors, and fiscal agents. These agents may or may not be health plans in their own right; for example, a health plan acting as another health plan's agent as another line of business. As stated earlier, a health plan that conducts HIPAA transactions through an agent is required to assure that the agent meets all HIPAA requirements that apply to the plan itself.

''Health plan'' includes the following, singly or in combination:

a. ''Group health plan'' (as currently defined by section 2791(a) of the Public Health Service Act). A group health plan is a plan that has 50 or more participants (as the term ''participant'' is currently defined by section 3(7) of ERISA) or is administered by an entity other than the employer that established and maintains the plan. This definition includes both insured and self-insured plans. We define ''participant'' separately below.

Section 2791(a)(1) of the Public Health Service Act defines ''group health plan'' as an employee welfare benefit plan (as defined in current section 3(1) of ERISA) to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, or otherwise.

b. ''Health insurance issuer'' (as currently defined by section 2791(b) of the Public Health Service Act).

Section 2791(b) of the Public Health Service Act currently defines a ''health insurance issuer'' as an insurance company, insurance service, or insurance organization that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance.

c. ''Health maintenance organization'' (as currently defined by section 2791(b) of the Public Health Service Act).

Section 2791(b) of the Public Health Service Act currently defines a ''health maintenance organization'' as a Federally qualified health maintenance organization, an organization recognized as such under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such a health maintenance organization. These organizations may include preferred provider organizations, provider sponsored organizations, independent practice associations, competitive medical plans, exclusive provider organizations, and foundations for medical care.

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

e. The Medicaid program (title XIX of the Act).

f. A ''Medicare supplemental policy'' as defined under section 1882(g)(1) of the Act.

Section 1882(g)(1) of the Act defines a ''Medicare supplemental policy'' as a health insurance policy that a private entity offers a Medicare beneficiary to provide payment for expenses incurred for services and items that are not reimbursed by Medicare because of deductible, coinsurance, or other limitations under Medicare. The statutory definition of a Medicare supplemental policy excludes a number of plans that are generally considered to be Medicare supplemental plans, such as health plans for employees and former employees and for members and former members of trade associations and unions. A number of these health plans may be included under the definitions of ''group health plan'' or ''health insurance issuer'', as defined in paragraphs a. and b. above.

g. A ''long-term care policy,'' including a nursing home fixed-indemnity policy. A ''long-term care policy'' is considered to be a health plan regardless of how comprehensive it is. We recognize the long-term care insurance segment of the industry is largely unautomated and we welcome comments regarding the impact of HIPAA on the long-term care segment.

h. An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers. This includes plans that are referred to as multiple employer welfare arrangements (''MEWAs'').

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

j. The veterans health care program under chapter 17 of title 38 of the United States Code.

This health plan primarily furnishes medical care through hospitals and clinics administered by the Department of Veterans Affairs for veterans with a service-connected disability that is compensable. Veterans with nonservice-connected disabilities (and no other health benefit plan) may receive health care under this health plan to the extent resources and facilities are available.

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

CHAMPUS primarily covers services furnished by civilian medical providers to dependents of active duty members of the uniformed services and retirees and their dependents under age 65.

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

This program furnishes services, generally through its own health care providers, primarily to persons who are eligible to receive services because they are of American Indian or Alaskan Native descent.

m. The Federal Employees Health Benefits Program under 5 U.S.C. chapter 89.

This program consists of health insurance plans offered to active and retired Federal employees and their dependents. Depending on the health plan, the services may be furnished on a fee-for-service basis or through a health maintenance organization.

(**Note:** Although section 1171(5)(M) of the Act refers to the ''Federal Employees Health Benefit Plan,'' this and any other rules adopting administrative simplification standards will use the correct name, the Federal Employees Health Benefits Program. One health plan does not cover all Federal employees; there are over 350 health plans that provide health benefits coverage to Federal employees, retirees, and their eligible family members. Therefore, we will use the correct name, the Federal Employees Health Benefits Program, to make clear that the administrative simplification standards apply to all health plans that participate in the Program.)

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

We would include a fourteenth category of health plan in addition to those specifically named in HIPAA, as there are health plans that do not readily fit into the other categories but whose major purpose is providing health benefits. The Secretary would determine which of these plans are health plans for purposes of title II of HIPAA. This category would include the Medicare Plus Choice plans that will become available as a result of section 1855 of the Act as amended by section 4001 of the Balanced Budget Act of 1997 (Public Law 105–33) to the extent that these health plans do not fall under any other category.

6. Small Health Plan

We would define a ''small health plan'' as a group health plan with fewer than 50 participants.

The HIPAA does not define a ''small health plan'' but instead leaves the definition to be determined by the Secretary. The Conference Report suggests that the appropriate definition of a ''small health plan'' is found in current section 2791(a) of the Public Health Service Act, which is a group health plan with fewer than 50 participants. We would also define small individual health plans as those with fewer than 50 participants.

7. Individually Identifiable Health Information

Section 1171(6) states the term ''individually identifiable health information'' means any information, including demographic information collected from an individual, that—

a. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

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

(i) Identifies the individual, or

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

8. Standard

Section 1171 of the Act defines ''standard,'' when used with reference to a data element of health information or a transaction referred to in section 1173(a)(1) of the Act, as any such data element or transaction that meets each of the standards and implementation specifications adopted or established by the Secretary with respect to the data element or transaction under sections 1172 through 1174 of the Act.

Under our definition, the security standard would be a set of requirements adopted or established to preserve and maintain the confidentiality and privacy of electronically stored, maintained, or transmitted health information promulgated either by an organization accredited by the ANSI or HHS.

9. Transaction

''Transaction'' would mean the exchange of information between two parties to carry out financial and administrative activities related to health care. A transaction would be (a) any of the transactions listed in section 1173(a)(2) of the Act, and (b) any determined appropriate by the Secretary in accordance with section 1173(a)(1)(B) of the Act. We present them below in the order in which we propose to list them in the regulations text.

A ''transaction'' would mean any of the following:

a. Health claims or equivalent encounter information. This transaction may be used to submit health care claim billing information, encounter information, or both, from health care providers to payers, either directly or via intermediary billers and claims clearinghouses.

b. Health care payment and remittance advice. This transaction may be used by a health plan to make a payment to a financial institution for a health care provider (sending payment only), to send an explanation of benefits remittance advice directly to a health care provider (sending data only), or to make payment and send an explanation of benefits remittance advice to a health care provider via a financial institution (sending both payment and data).

c. Coordination of benefits. This transaction set can be used to transmit health care claims and billing payment information between payers with different payment responsibilities where coordination of benefits is required or between payers and regulatory agencies to monitor the furnishing, billing, and/or payment of health care services within a specific health care/insurance industry segment.

In addition to the nine electronic transactions specified in section 1173(a)(2) of the Act, section 1173(f) directs the Secretary to adopt standards for transferring standard data elements among health plans for coordination of benefits. This particular provision does not state that these should be standards for electronic transfer of standard data elements among health plans. However, we believe that the Congress, when writing this provision, intended for these standards to be an electronic form of transactions for coordination of benefits and sequential processing of claims. The Congress expressed its intent on these matters generally in section 1173(a)(1)(B) of the Act, where the Secretary is directed to adopt ''other financial and administrative transactions * * * consistent with the goals of improving the operation of the health care system and reducing administrative costs.''

d. Health claim status. This transaction may be used by health care providers and recipients of health care products or services (or their authorized agents) to request the status of a health care claim or encounter from a health plan.

e. Enrollment and disenrollment in a health plan. This transaction may be used to establish communication between the sponsor of a health benefit and the payer. It provides enrollment data, such as subscriber and dependents, employer information, and primary care health care provider information. A sponsor is the backer of the coverage, benefit, or product. A sponsor can be an employer, union, government agency, association, or insurance company. The health plan refers to an entity that pays claims, administers the insurance product or benefit, or both.

f. Eligibility for a health plan. This transaction may be used to inquire about the eligibility, coverage, or benefits associated with a benefit plan, employer, plan sponsor, subscriber, or a dependent under the subscriber's policy. It also can be used to communicate information about or changes to eligibility, coverage, or benefits from information sources (such as insurers, sponsors, and payers) to information receivers (such as physicians, hospitals, third party administrators, and government agencies).

g. Health plan premium payments. This transaction may be used by, for example, employers, employees, unions, and associations to make and keep track of payments of health plan premiums to their health insurers. This transaction may also be used by a health care provider, acting as liaison for the beneficiary, to make payment to a health insurer for coinsurance, copayments, and deductibles.

h. Referral certification and authorization. This transaction may be used to transmit health care service referral information between health care providers, health care providers furnishing services, and payers. It can also be used to obtain authorization for certain health care services from a health plan.

i. First report of injury. This transaction may be used to report information pertaining to an injury, illness, or incident to entities interested in the information for statistical, legal, claims, and risk management processing requirements.

j. Health claims attachments. This transaction may be used to transmit health care service information, such as subscriber, patient, demographic, diagnosis, or treatment data for the purpose of a request for review, certification, notification, or reporting the outcome of a health care services review.

k. Other transactions as the Secretary may prescribe by regulation.

Under section 1173(a)(1)(B) of the Act, the Secretary may adopt standards, and data elements for those standards, and for other financial and administrative transactions deemed appropriate by the Secretary. These transactions would be consistent with the goals of improving the operation of the health care system and reducing administrative costs.

C. Effective Dates—General

[Please label written comments or e-mailed comments about this section with the subject: effective dates]

In general, any given standard would be effective 24 months after the effective date (36 months for small health plans) of the final rule for that standard. Because there are other standards to be established than those in this proposed rule, we specify the date for a given standard under the subpart for that standard.

Health plans would be required by part 142 to comply with our requirements as follows:

1. Each health plan that is not a small plan would have to comply with the requirements of part 142 no later than 24 months after the effective date of the final rule.

2. Each small health plan would have to comply with the requirements of part 142 no later than 36 months after the effective date of the final rule.

Health care providers and health care clearinghouses would be required to begin using the standard by 24 months after the effective date of the final rule. (The effective date of the final rule will be 60 days after the final rule is published in the **Federal Register**.)

Provisions of trading partner agreements that stipulate data content, format definitions, or conditions that conflict with the adopted standard would be invalid beginning 36 months from the effective date of the final rule for small health plans, and 24 months from the effective date of the final rule for all other health plans.

If the HHS adopts a modification to an implementation specification or a standard, the implementation date of the modification would be no earlier than the 180th day following the adoption of the modification. HHS would determine the actual date, taking into account the time needed to comply due to the nature and extent of the modification. HHS would be able to extend the time for compliance for small health plans. This provision would be at § 142.106.

Any of the health plans, health care clearinghouses, and health care providers may implement a given standard earlier than the date specified in the subpart created for that standard. We realize that this may create some problems temporarily, as early implementers would have to be able to continue using old standards until the new one must, by law, be in place.

D. Security Standard

[Please label written comments or e-mailed comments about this section with the subject: Security Standard—General]

Section 142.308 would set forth the security standard. There is no recognized single standard that integrates all the components of security (administrative procedures, physical safeguards, technical security services, and technical mechanisms) that must be in place to preserve health information confidentiality and privacy as defined in the law. Therefore, we are designating a new, comprehensive standard, which defines the security requirements to be fulfilled.

In fact, there are numerous security guidelines and standards in existence today, focusing on the different techniques available for implementing the various aspects of security. We thoroughly researched the existing guidelines and standards, and consulted extensively with the organizations that developed them. A list of the organizations with which we consulted can be found in section G. below. As a result of these consultations and our research, we identified several high-level concepts on which the standard is based:

- The standard must be comprehensive.
- Consultation with standards development organizations, such as ANSI-accredited organizations, as well as business interest organizations, revealed the need for a standard that addressed all aspects of security in a concerted fashion. The HISB noted in its report to the Secretary that:

''Comprehensive adoption of security standards in health care, not piecemeal implementation, is advocated to provide security to data that is exchanged between health care entities.

By definition, if a system or communications between two systems, were implemented with technology(s) meeting standards in a general system security framework (Identification and Authentication; Authorization and Access Control; Accountability; Integrity and Availability; Security of Communication; and Security Administration.) that system would be essentially secure.

* * * no single standards development organization (SDO) is addressing all aspects of health care information security and confidentiality, and specifically, no single SDO is developing standards that cover every category of the security framework.'' [Page 189]

- The standard must be technology-neutral.

Our proposed standard does not reference or advocate specific technology because security technology is changing quickly. We want to give providers/plans/clearinghouses flexibility to choose their own technical solutions. A standard that is dependent on a specific technology or technologies would not be flexible enough to use future advances.

- The standard must be scalable.

The standard must be able to be implemented by all the affected entities, from the smallest provider to the largest clearinghouse. A single approach would be neither economically feasible nor effective in safeguarding health data. For example, in a small physician practice, a contingency plan for system emergencies might be only a few pages long, and cover issues such as where backup diskettes must be stored, and the location of a backup personal computer (PC). At a large health plan, the contingency plan might consist of multiple volumes and cover issues such as remote hot site operations and secure off-site storage of electronic media. The physician office solution would not protect the large plan's data, and the plan's solution would not be economically feasible (or necessary) for the physician office. Moreover, the statute specifically directed the Secretary to take into account the needs and capabilities of small and rural health care providers, as those terms are defined by the Secretary. The scalability of our approach addresses this direction. We are not proposing specific definitions of ''small'' and ''rural'' health care providers because the statute provides no exemptions or special benefits for these two groups. However, we solicit comments on the necessity to define these terms.

General Approach

We would define the security standard as a set of requirements with implementation features that providers, plans, and clearinghouses must include in their operations to assure that electronic health information pertaining to an individual remains secure. The implementation features address specific aspects of the requirements. The standard does not reference or advocate specific technology. This would allow the security standard to be stable, yet flexible enough to take advantage of state-of-the-art technology.

The standard does not address the extent to which a particular entity should implement the specific features. Instead, we would require that each affected entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its business requirements. How individual security requirements would be satisfied and which technology to use would be business decisions that each organization would have to make.

The recommendations contained in the National Research Council's 1997 report *For The Record: Protecting Electronic Health Information* support our approach to the development of a security standard. This report presents findings and recommendations related to health data security, and is widely viewed as an authoritative and comprehensive source on the subject. The report concludes that appropriate security practices are highly dependent on individual circumstances, but goes on to suggest that:

> ''It is therefore not possible to prescribe in detail specific practices for all organizations; rather, each organization must analyze its systems, vulnerabilities, risks, and resources to determine optimal security measures. Nevertheless, the committee believes that a set of practices can be articulated in a sufficiently general way that they can be adopted by all health care organizations in one form or another.'' (Page 168)

The specific requirements and supporting implementation features detailed in the next section represent this general set of practices. Many health care entities have already implemented some or all of these practices. We believe they represent those practices that are necessary in order to conduct business electronically in the health care industry today and, therefore, are normal business costs.

Inherent in this approach is a balance between the need to secure health data against risk and the economic cost of doing so. Health care entities must consider both aspects in devising their security solutions.

Specific Requirements

The proposed standard requires that each health care entity engaged in electronic maintenance or transmission of health information assess potential risks and vulnerabilities to the individual health data in its possession in electronic form, and develop, implement, and maintain appropriate security measures. Most importantly, these measures must be documented and kept current.

The proposed security standard consists of the requirements that a health care entity must address in order to safeguard the integrity, confidentiality, and availability of its electronic data. It also describes the implementation features that must be present in order to satisfy each requirement. The proposed requirements and implementation features were developed by the implementation team based on knowledge of security procedures and existing standards and guidelines described above. This was an iterative process that involved extensive outreach with a number of health care industry and Department of Commerce security experts. We also drew upon Recommendations 1 and 3 in the National Research Council's 1997 report, *For The Record*, that were recommended for immediate implementation.

''Recommendation 1: All organizations that handle patient-identifiable health care information—regardless of size—should adopt the set of technical and organizational policies, practices, and procedures described below to protect such information.''

The proposed security standard addresses the following policies, practices, and procedures that were listed under Recommendation 1:

- Organizational Practices
  1. Security and confidentiality policies
  2. Information security officers
  3. Education and training programs, and
  4. Sanctions
- Technical Practices and Procedures
  1. Individual authentication of users
  2. Access controls
  3. Audit trails
  4. Physical security and disaster recovery
  5. Protection of remote access points
  6. Protection of external electronic communications
  7. Software discipline, and
  8. System assessment

''Recommendation 3: The federal government should work with industry to promote and encourage an informed public debate to determine an appropriate balance between the primary concerns of patients and the information needs of various users of health care information.''

This proposed security standard was developed in the spirit of Recommendation 3. The security standard development process has been an open one with invitations to a number of organizations to participate in the security discussions. Although implementation team membership was limited to government employees, nongovernmental organizations; business organizations; individuals knowledgeable in security; and educational institutions have been encouraged to express their views.

As a result of the collaborative security regulation development process, the implementation team has chosen to divide the proposed security requirements, for purposes of presentation only, into the following four categories:

- Administrative procedures to guard data integrity, confidentiality, and availability—these are documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data.
- Physical safeguards to guard data integrity, confidentiality, and availability—these relate to the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures used to control access to computer systems and facilities.
- Technical security services to guard data integrity, confidentiality, and availability—these include the processes that are put in place to protect and to control and monitor information access, and
- Technical security mechanisms—these include the processes that are put in place to prevent unauthorized access to data that is transmitted over a communications network.

It should be noted that the only necessity is that the requirements would be met, not that they be presented in these four categories. Under this proposed rule, a business entity could choose to order the requirements in any manner that suits its business.

We then determined the requirements and implementation features that health plans, providers, and clearinghouses would implement. The implementation features describe the requirements in greater detail. Some requirements do not require this additional level of detail. Within the four categories, the requirements and implementation features are presented in alphabetical order to ensure that no one item is considered to be more important than another. The relative importance of the requirements and implementation features would depend on the characteristics of each organization.

The four categories of the matrix are described in greater detail in § 142.308 and are depicted in tabular form along with the electronic signature standard in

a combined matrix located at Addendum 1. We have not included the matrix in the proposed regulation text. We invite your comments concerning the appropriateness and usefulness of including the matrix in the final regulation text. We also solicit comments as to the level of detail expressed in requirement implementation features; i.e., do any represent a level of detail that goes beyond what is necessary or appropriate. We have also provided a glossary of terms to facilitate a common understanding of the matrix entries. The glossary can be found at Addendum 2. Finally, we have included currently existing standards and guidelines mapped to the proposed security standard. This mapping is not all inclusive and is located at Addendum 3.

1. Administrative Procedures

[Please label written comments or e-mailed comments about this section with the subject: administrative procedures]

In this proposed rule, the administrative requirements and supporting implementation features are presented at § 142.308(a). We would require each to be documented. We would require the documentation to be made available to those individuals responsible for implementing the procedures and would require it to be reviewed and updated periodically. The following matrix depicts the requirements and supporting implementation features for the Administrative Procedures category. Following the matrix is a discussion of each of the requirements under that category.

ADMINISTRATIVE PROCEDURES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation
Certification	
Chain of trust partner agreement	
Contingency plan (all listed implementation features must be implemented).	Applications and data criticality analysis. Data backup plan. Disaster recovery plan. Emergency mode operation plan. Testing and revision.
Formal mechanism for processing records	
Information access control (all listed implementation features must be implemented).	Access authorization. Access establishment. Access modification.
Internal audit	
Personnel security (all listed implementation features must be implemented).	Assure supervision of maintenance personnel by authorized, knowledgeable person. Maintenance of record of access authorizations. Operating, and in some cases, maintenance personnel have proper access authorization. Personnel clearance procedure. Personnel security policy/procedure. System users, including maintenance personnel, trained in security.
Security configuration mgmt. (all listed implementation features must be implemented).	Documentation. Hardware/software installation & maintenance review and testing for security features. Inventory. Security Testing. Virus checking.
Security incident procedures (all listed implementation features must be implemented).	Report procedures. Response procedures.
Security management process (all listed implementation features must be implemented).	Risk analysis. Risk management. Sanction policy. Security policy.
Termination procedures (all listed implementation features must be implemented).	Combination locks changed. Removal from access lists. Removal of user account(s). Turn in keys, token or cards that allow access.
Training (all listed implementation features must be implemented)	Awareness training for all personnel (including mgmt) Periodic security reminders. User education concerning virus protection. User education in importance of monitoring log in success/failure, and how to report discrepancies. User education in password management

a. *Certification.* Each organization would be required to evaluate its computer system(s) or network design(s) to certify that the appropriate security has been implemented. This evaluation could be performed internally or by an external accrediting agency.

We are, at this time, soliciting input on appropriate mechanisms to permit independent assessment of compliance. We would be 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 solicit comments on the extent to which obtaining external certification would create an undue burden on small or rural providers.

b. *Chain of Trust Partner Agreement.* If data are processed through a third party, the parties would be required to enter into a chain of trust partner agreement. This is a contract in which the parties agree to electronically exchange data and to protect the transmitted data. The sender and receiver are required and depend upon each other to maintain the integrity and confidentiality of the transmitted information. Multiple two-party contracts may be involved in moving information from the originating party to the ultimate receiving party. For example, a provider may contract with a clearinghouse to transmit claims to the clearinghouse; the clearinghouse, in turn, may contract with another clearinghouse or with a payer for the further transmittal of those claims. These agreements are important so that the same level of security will be maintained at all links in the chain when information moves from one organization to another.

c. *Contingency Plan.* We would require a contingency plan to be in effect for responding to system emergencies. The organization would be required to perform periodic backups of data, have available critical facilities for continuing operations in the event of an emergency, and have disaster recovery procedures in place. To satisfy the requirement, the plan would include the following:

- Applications and data criticality analysis,
- A data backup plan,
- A disaster recovery plan,
- An emergency mode operation plan, and
- Testing and revision procedures.

d. *Formal Mechanism for Processing Records* There would be a formal mechanism for processing records, that is, documented policies and procedures for the routine and nonroutine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information. This is important to limit the inadvertent loss or disclosure of secure information because of process issues.

e. *Information Access Control.* An entity would be required to establish and maintain formal, documented policies and procedures for granting different levels of access to health care information. To satisfy this requirement, the following features would be provided:

- Access authorization policies and procedures.
- Access establishment policies and procedures.
- Access modification policies and procedures.

Access control is also discussed later in this document in the personnel security requirement and under the physical safeguards, technical security services, and technical security mechanisms categories.

f. *Internal Audit.* There would be a requirement for an ongoing internal audit process, which is the in-house review of the records of system activity (for example, logins, file accesses, security incidents) maintained by an entity. This is important to enable the organization to identify potential security violations.

g. *Personnel Security.* There would be a requirement that all personnel with access to health information must be authorized to do so after receiving appropriate clearances. This is important to prevent unnecessary or inadvertent access to secure information. The personnel security requirement would require entities to meet the following conditions:

- Assure supervision of personnel performing technical systems maintenance activities by authorized, knowledgeable persons.
- Maintain access authorization records.
- Insure that operating, and in some cases, maintenance personnel have proper access.
- Employ personnel clearance procedures
- Employ personnel security policy/procedures.
- Ensure that system users, including technical maintenance personnel are trained in system security.

h. *Security Configuration Management.* The organization would be required to implement measures, practices, and procedures for the security of information systems. These would be coordinated and integrated with other system configuration management practices in order to create and manage system integrity. This integration process is important to ensure that routine changes to system hardware and/or software do not contribute to or create security weaknesses. This requirement would include the following:

- Documentation.
- Hardware/software installation and maintenance review and testing for security features.
- Inventory procedures.
- Security testing.
- Virus checking.

i. *Security Incident Procedures.* There would be a requirement to implement accurate and current security incident procedures. These are formal, documented instructions for reporting security breaches, so that security violations are reported and handled promptly. These instructions would include the following:

- Report procedures.
- Response procedures.

j. *Security Management Process.* A process for security management would be required. This involves creating, administering, and overseeing policies to ensure the prevention, detection, containment, and correction of security breaches. We would require the organization to have a formal security management process in place to address the full range of security issues. Security management includes the following mandatory implementation features:

- Risk analysis.
- Risk management.
- A sanction policy.
- A security policy.

k. *Termination Procedures.* There would be a requirement to implement termination procedures, which are formal, documented instructions, including appropriate security measures, for the ending of an employee's employment or an internal/external user's access. These procedures are important to prevent the possibility of unauthorized access to secure data by those who are no longer authorized to access the data. Termination procedures would include the following mandatory implementation features:

- Changing combination locks.
- Removal from access lists.
- Removal of user account(s).
- Turn in of keys, tokens, or cards that allow access.

1. *Training.* This proposed rule would require security training for all staff regarding the vulnerabilities of the health information in an entity's possession and procedures which must be followed to ensure the protection of that information. This is important because employees need to understand their security responsibilities and make security a part of their day-to-day activities. The implementation features that would be required to be incorporated follow:

- Awareness training for all personnel, including management, (this is also included as a requirement under physical safeguards).
- Periodic security reminders.
- User education concerning virus protection.
- User education in importance of monitoring login success/failure, and how to report discrepancies.
- User education in password management.

2. Physical Safeguards To Guard Data Integrity, Confidentiality, and Availability

[Please label written comments or e-mailed comments about this section with the subject: Physical Safeguards]

The requirements and implementation features for physical safeguards are presented at § 142.308(b) of this proposed rule. We would require each of these safeguards to be documented. We would require this documentation to be made available to those individuals responsible for implementing the safeguards and to be reviewed and updated periodically. The following matrix depicts the requirements and implementation features for the Physical Safeguards category. Following the matrix is a discussion of each of the requirements under that category.

PHYSICAL SAFEGUARDS TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation
Assigned security responsibility	
Media controls (all listed implementation features must be implemented).	Access control. Accountability (tracking mechanism). Data backup. Data storage. Disposal.
Physical access controls (limited access) (all listed implementation features must be implemented).	Disaster recovery. Emergency mode operation. Equipment control (into and out of site). Facility security plan. Procedures for verifying access authorizations prior to physical access. Maintenance records. Need-to-know procedures for personnel access. Sign-in for visitors and escort, if appropriate. Testing and revision.
Policy/guideline on work station use	
Secure work station location	
Security awareness training.	

a. *Assigned Security Responsibility.* We would require the security responsibility to be assigned to a specific individual or organization, and the assignment be documented. These 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. This assignment is important to provide an organizational focus and importance to security and to pinpoint responsibility.

b. *Media Controls.* Media controls would be required in the form of formal, documented policies and procedures that govern the receipt and removal of hardware/software (for example, diskettes, tapes) into and out of a facility. They are important to ensure total control of media containing health information. These controls would include the following mandatory implementation features:

- Controlled access to media.
- Accountability (tracking mechanism).
- Data backup.
- Data storage.
- Disposal.

c. *Physical Access Controls.* Physical access controls (limited access) would be required. These would be formal, documented policies and procedures for limiting physical access to an entity while ensuring that properly authorized access is allowed. These controls would be extremely important to the security of health information by preventing unauthorized physical access to information and ensuring that authorized personnel have proper access. These controls would include the following mandatory implementation features:

- Disaster recovery.
- Emergency mode operation.
- Equipment control (into and out of site).
- A facility security plan.
- Procedures for verifying access authorizations prior to physical access.
- Maintenance records.
- Need-to-know procedures for personnel access.
- Sign-in for visitors and escort, if appropriate.
- Testing and revision.

d. *Policy/Guideline on Workstation Use.* Each organization would be required to have a policy/guideline on workstation use. These documented instructions/procedures would delineate the proper functions to be performed and the manner in which those functions are to be performed (for example, logging off before leaving a terminal unattended). This would be important so that employees will understand the manner in which workstations must be used to maximize the security of health information.

e. *Secure Workstation Location.* Each organization would be required to put in place physical safeguards to eliminate or minimize the possibility of unauthorized access to information. This would be important especially in public buildings, provider locations, and in areas where there is heavy pedestrian traffic.

f. *Security Awareness Training.* Security awareness training would be required for all employees, agents, and contractors. This would be important because employees would need to understand their security responsibilities based on their job responsibilities in the organization and make security a part of their daily activities.

3. Technical Security Services To Guard Data Integrity, Confidentiality, and Availability

[Please label written comments or e-mailed comments about this section with the subject: Technical Security Services]

The proposed requirements and implementation features for technical security services are presented at § 142.308(c). We would require each of these services to be implemented and documented. The documentation would be made available to those individuals responsible for implementing the services and would be reviewed and updated periodically. The following matrix depicts the requirements and implementation features for the Technical Security Services category. Following the matrix is a discussion of

each of the requirements under that category.

TECHNICAL SECURITY SERVICES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation
Access control (The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context-based access, Role-based access, User-based access. The use of Encryption is optional).	Context-based access. Encryption. Procedure for emergency access. Role-based access. User-based access.
Audit controls	
Authorization control (At least one of the listed implementation features must be implemented).	Role-based access. User-based access.
Data Authentication	
Entity authentication (The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented).	Automatic logoff. Biometric. Password. PIN. Telephone callback. Token. Unique user identification.

a. *Access Control.* There would be a requirement for access control which would restrict access to resources and allow access only by privileged entities. It would be important to limit access to health information to those employees who have a business need to access it. Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, classification, and subject-object separation. The following implementation feature would be used:

- Procedure for emergency access.

In addition, at least one of the following three implementation features would be used:

- Context-based access.
- Role-based access.
- User-based access.

The use of the encryption implementation feature would be optional.

b. *Audit Controls.* Each organization would be required to put in place audit control mechanisms to record and examine system activity. They would be important so that the organization can identify suspect data access activities, assess its security program, and respond to potential weaknesses.

c. *Authorization Control.* There would be a requirement to put in place a mechanism for obtaining consent for the use and disclosure of health information. These controls would be necessary to ensure that health information is used only by properly authorized individuals. Either of the following implementation features may be used:

- Role-based access.
- User-based access (see access control, above.).

d. *Data Authentication.* Each organization would be required to be able to provide corroboration that data in its possession has not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, double keying, a message authentication code, or digital signature.

e. *Entity Authentication.* Each organization would be required to implement entity authentication, which is the corroboration that an entity is who it claims to be. Authentication would be important to prevent the improper identification of an entity who is accessing secure data. The following implementation features would be used:

- Automatic log off.
- Unique user identification.

In addition, at least one of the following implementation features would be used:

- A biometric identification system.
- A password system.
- A personal identification number (PIN).
- Telephone callback.
- A token system which uses a physical device for user identification.

4. Technical Security Mechanisms To Guard Against Unauthorized Access to Data That Is Transmitted Over a Communications Network

[Please label written comments or e-mailed comments about this section with the subject: Technical Security Mechanisms]

In this proposed rule, the requirements and implementation features for technical security mechanisms are presented at § 142.308(d). Each of these mechanisms would need to be documented. The documentation would be made available to those individuals responsible for implementing the mechanisms and would be reviewed and updated periodically. The following matrix depicts the requirement and implementation features for the Technical Security Mechanisms category. Following the matrix is a discussion of the requirement under that category.

TECHNICAL SECURITY MECHANISMS TO GUARD AGAINST UNAUTHORIZED ACCESS TO DATA THAT IS TRANSMITTED OVER A COMMUNICATIONS NETWORK

Requirement	Implementation
Communications/network controls (If communications or networking is employed, the following implementation features must be implemented: Integrity controls, Message authentication. In addition, one of the following implementation features must be implemented: Access controls, Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting).	Access controls. Alarm. Audit trail. Encryption. Entity authentication. Event reporting. Integrity controls. Message authentication.

Each organization that uses communications or networks would be required to protect communications containing health information that are transmitted electronically over open networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient, and to protect their information systems from intruders trying to access systems through external communication points. When using open networks, some form of encryption should be employed. The utilization of less open systems/networks such as those provided by a value-added network (VAN) or private-wire arrangement provides sufficient access controls to allow encryption to be an optional feature. These controls would be important because of the potential for compromise of information over open systems such as the Internet or dial-in lines.

The following implementation features would be in place:

- Integrity controls.
- Message authentication.

One of the following implementation features would be in place:

- Access controls.
- Encryption.

In addition, if using a network for communications, the following implementation features would be in place:

- Alarm.
- Audit trail.
- Entity authentication.
- Event reporting.

Small or Rural Provider Example. The size and organizational structure of the entities that would be required to implement this standard vary tremendously. Therefore, it would be impossible to provide examples that would cover every possible implementation of security in the health care industry. Nevertheless, we have included an example describing the manner in which a small or rural provider might choose to implement the requirements of the standard. (For purposes of this example, we would describe a small or rural provider as a one to four physician office, with two to five additional employees. The office uses a PC-based practice management system, which is used to communicate intermittently with a clearinghouse for submission of electronic claims. The number of providers is of less importance for this example than the relatively simple technology in use and the fact that there is insufficient volume or revenue to justify employment of a computer system administrator.) We want to emphasize that there are numerous ways in which an entity could implement these requirements and features. This example does not necessarily represent the best way or the only way in which an entity could choose to implement security.

We anticipate that the small or rural provider office, as described above, would normally evaluate and self-certify that the appropriate security is in place for its computer system and office procedures. This evaluation could be done by a knowledgeable person on the staff, or more likely, by a consultant or by the vendor of the practice management system as a service to its customers. First, the office might assess actual and potential risks to its information assets. Then, to establish appropriate security, the office would develop policies and procedures to mitigate and manage those risks. These would include an overall framework outlining information security activities and responsibilities, and repercussions for failure to meet those responsibilities.

Next, this office might develop contingency plans to reduce or negate the damage resulting from processing anomalies; for example, establish a routine process for maintaining back up floppy disks at a second location, obtain a PC maintenance contract, and arrange for use of a backup PC should the need arise. This office would need to periodically review its plan to determine whether it still met the office's needs.

The office would need to create and document a personnel security policy and procedures to be followed. A key individual on the office staff should be charged with the responsibility for assuring the Personnel Security requirement is met. This responsibility would include seeing that the access authorization levels granted are documented and kept current (for example, records are kept of everyone who is permitted to use the PC and what files they may access), and training all personnel in security. Again, we emphasize that these requirements are scalable. The requirement for Personnel Clearance Procedures could be met in a small office with standard personal and professional reference checks, while a large organization may employ more formal, rigorous background investigations.

This same individual could also be charged with the responsibility for Security Configuration Management and Termination Procedures. For our small provider, the Security Configuration Management requirement would be relatively easy to satisfy; the necessary features could be part of a purchased hardware/software package (for example, a new PC might be equipped with virus checking software), or included as part of the support supplied with the purchase of equipment and software. Termination procedures would incorporate specific security actions to be taken as a result of an employee's termination, such as obtaining all keys and changing combinations or passwords. A ''position description'' document describing this person's duties could specify the level of detail necessary.

The small or rural provider office would also need to ensure that they have activated the internal auditing capability of the software used to manage health data files so that it tracks who has accessed the data. (We expect that the capability of keeping audit trails will become standard in all health care software in the near future, spurred on by the health information privacy debates in the Congress and elsewhere.)

A small or rural provider may document compliance with many of the

foregoing administrative security requirements by including them in an ''office procedures'' type of document that should be required reading by new employees and always available for reference. Requirements that would lend themselves to inclusion in an ''office procedures'' document include: contingency plans, formal records processing procedures, information access controls (rules for granting access, actual establishment of access, and procedures for modifying such access), security incident procedures (for example, who is to be notified if it appears that medical information has been accessed by an unauthorized party), and training. Periodic security reminders could include visual aids, such as posters and screen savers, and oral reminders in recurring meetings.

Physical Access controls would be relatively straightforward for this small or rural office, using locked rooms and/or closets to secure equipment and media from unauthorized access. The ''office procedures/policies'' manual should include directions for authorizing access and keeping records of authorized accesses. Media Controls and Workstation Use policy instructions would be developed by the office and would include additional instructions on such items as where to store backed-up data, how to dispose of data no longer needed, or logging off when leaving terminals unattended.

Safeguards for the security of workstation location(s) would depend upon the physical surroundings in the small or rural office. Our small or rural provider may meet the requirements by locating equipment in areas that are generally populated by office staff and have some degree of physical separation from the public. Security Awareness Training would be part of the new employee orientation process and would be a periodic recurring discussion item in staff meetings.

The Technical Security Services requirements for Access Control, Entity Authentication, and Authorization Control may be achieved simply by implementing a user-based data access model (assigning a user-name and password combination to each authorized employee). Other access models could be employed if desired, but would prove unwieldy for the small office. For example, the role-based access process groups users with similar data access needs, and context-based access is based upon the context of a transaction—not on the attributes of the initiator. By assigning full access rights to a minimum of two key individuals in the office, implementation of the Emergency Access feature could be satisfied. Audit control mechanisms, by necessity, would be provided by software featuring that capability. By establishing and using a message authentication code, Data Authentication would be achieved. Use of the password system mentioned above could also satisfy the Unique User Identification requirement.

As our example provider contracts with a third party to handle claims processing, the claims processing contract would be the vehicle to provide for a chain of trust (requiring the contractor to implement the same security requirements and take responsibility for protecting the data it receives).

If this provider chooses to use the Internet to transmit or receive health information, some form of encryption must be used. For example, the provider could procure and use commercial software to provide protection against unauthorized access to the data transmitted or received. (This decision must take into account what encryption system the message recipient uses.) On the other hand, health information when transmitted via other means such as VANs, private wires, or even dial-up connections may not require such absolute protection as is provided by encryption. This small or rural provider would likely not be part of a network configuration, therefore, only integrity controls and message authentication would be required and could be provided by currently available software products, most likely provided as part of their contract with their health care clearinghouse.

Small providers may need guidance regarding the content of the documents required by this rule (for example, specifics of a chain of trust partner agreement). We would expect models of the documentation discussed in this example to be developed by industry associations and vendors. If this model documentation is not developed, DHHS would work with the industry to develop them.

E. Electronic Signature Standard

[Please label written comments or e-mailed comments about this section with the subject: Electronic Signature Standard]

HIPAA directs the Secretary of the Department of Health and Human Services to coordinate with the Secretary of the Department of Commerce in adopting standards for the electronic transmission and authentication of signatures with respect to the transactions referred to in the law. This rule was developed in coordination with the Department of Commerce's National Institute of Standards and Technology. We propose to adopt a cryptographically based digital signature as the standard.

Whenever a HIPAA specified transaction requires the use of an electronic signature, the standard must be used. It should be noted that an electronic signature is not required for any of the currently proposed standard transactions.

In the electronic environment, the same legal weight associated with an original signature on a paper document may be needed for electronic data. Use of an electronic signature refers to the act of attaching a signature by electronic means. The electronic signature process involves authentication of the signer's identity, a signature process according to system design and software instructions, binding of the signature to the document and non-alterability after the signature has been affixed to the document. The generation of electronic signatures requires the successful identification and authentication of the signer at the time of the signature.

The proposed standard for electronic signature is presented at § 142.310 and would be digital.

The following matrix depicts the requirement and implementation features for electronic signatures. Following the matrix is a discussion of the electronic signature requirement.

ELECTRONIC SIGNATURE

Requirement	Implementation
Digital signature (If digital signature is employed, the following three implementation features must be implemented: Message integrity, Nonrepudiation, User authentication. Other implementation features are optional).	Ability to add attributes. Continuity of signature capability. Countersignatures. Independent verifiability. Interoperability. Message integrity. Multiple Signatures. Nonrepudiation. Transportability. User authentication.

Various technologies may fulfill one or more of the requirements specified in the matrix. Authentication systems (passwords, biometrics, physical feature authentication, behavioral actions and token-based authentication) can be combined with cryptographic techniques to form an electronic signature. However, a complete electronic signature system may require more than one of the technologies mentioned above. If electronic signatures would be used, certain implementation features must be included, specifically:

- Message integrity.
- Nonrepudiation.
- User authentication.

Currently there are no technically mature techniques that provide the security service of nonrepudiation in an open network environment, in the absence of trusted third parties, other than digital signature-based techniques. Therefore, if electronic signatures are employed, we would require that digital signature technology be used. A digital signature is formed by applying a mathematical function to the electronic document. This process yields a unique bit string, referred to as a message digest. The digest (only) is encrypted using the originator's private key and the resulting bit stream is appended to the electronic document. The recipient of the transmitted document decrypts the message digest with the originator's public key, applies the same message hash function to the document, then compares the resulting digest with the transmitted version. If they are identical, then the recipient is assured that the message is unaltered and the identity of the signer is proven. Since only the signatory authority can hold the Private Key used to digitally sign the document, the critical feature of nonrepudiation is enforced. Other electronic signature implementation features that may be used follow:

- Ability to add attributes.
- Continuity of signature capability.
- Countersignatures capability.
- Independent verifiability.
- Interoperability.
- Multiple signatures.
- Transportability.

This standard is described in greater detail in § 142.310 of the regulation text and is depicted in tabular form along with the security standard in a combined matrix located at Addendum 1. We have not included the matrix in the proposed regulation text. We invite your comments concerning the appropriateness and usefulness of including the matrix in the final regulation text. We have also provided a glossary of terms to facilitate a common understanding of the matrix entries. The glossary can be found at Addendum 2. Finally, we have included currently existing standards and guidelines mapped to the proposed electronic signature standard. This mapping is not all inclusive and is located at Addendum 3.

F. Selection Criteria

Each individual implementation team weighted the criteria described in section I.B. above, Process for Developing National Standards, in terms of the standard it was addressing. As we assessed security and electronic signatures, it became apparent that while the security standard set forth in § 142.308 and the electronic signature standard set forth in § 142.310 satisfy all the criteria described above, they most strongly address criteria 1, 3, 7, 9, and 10. These criteria are described below in the specific context of these standards.

1. Improve the efficiency and effectiveness of the health care system.

The security and electronic signature standards would be integrated with the electronic transmission of health care information to improve the overall effectiveness of the health care system. This integration would assure that electronic health care information would not be accessible to any unauthorized person or organization, but would be both accurate and available to those who are authorized to receive it.

3. Be consistent and uniform with the other HIPAA standards and, secondly, with other private and public sector health data standards.

The security and electronic signature standards were developed after a comprehensive review of existing standards and guidelines, with significant input by a wide range of industry experts. As indicated in Addendum 3, the standards map well to existing standards and guidelines.

7. Be technologically independent of computer platforms and transmission protocols.

We have defined the security and electronic signature standards in terms of requirements that would allow businesses in the health care industry to select the technology that best meets their business requirements while still allowing them to comply with the standards.

9. Keep data collection and paperwork burdens on users as low as is feasible.

The security and electronic signature standards would allow individual health care industry businesses to ascertain the level of security information that would be needed. The confidentiality level associated with individual data elements concerning health care information would determine the appropriate security application to be used. The security standard would define the requirements to be met to achieve the privacy and confidentiality goal, but each business entity, driven by its business requirements, would decide what techniques and controls would provide appropriate and adequate electronic data protection. This would allow data collection and the paperwork burden to be as low as is feasible.

10. Incorporate flexibility to adapt more easily to changes in the health care infrastructure and information technology.

A technologically neutral security standard would be more adaptable to changes in infrastructure and information technology.

G. Consultations

In the development of the security and electronic signature standards, we consulted with many organizations, including those the legislation requires (section 1172(c)(3)(B) of the Act):

1. The NCVHS held two days of public hearings on security issues in August 1997, and made a recommendation to the Secretary of HHS, as required by the legislation. The NCVHS recommendation to the Secretary of HHS, as required by the legislation, was for a technologically neutral standard. It identified certain criteria to be established for a health information system to be secure. The proposed security standard complies with the NCVHS security recommendation.

2. The ANSI Accredited Standards Committee (ASC) X12 subcommittees on communication and control, insurance and government were contacted. Their current standards development effort is focused on messaging rather than on security requirements.

3. American Society for Testing and Materials (ASTM), Committee E31 on Computerized Systems participated in the security discussions.

4. Association for Electronic Health Care Transactions (AFEHCT), the clearinghouse organization, provided information on its health care transaction process requirements and emphasized that the security standard must be adaptable to different business needs.

5. Computer-based Patient Record Institute (CPRI) was consulted because the Work Group on Confidentiality, Privacy and Security is working on the establishment of guidelines, confidentiality agreements, security requirements, and frameworks. CPRI works closely with accredited standards development organizations.

6. Health Level Seven (HL–7) has been contacted through its participation at the HISB meetings.

7. NUCC and the NUBC were apprised of the different implementation teams' efforts. NUBC has not addressed security issues at any of the public meetings. NUCC identified a number of issues at its November 18–19 meeting and provided written comments to us.

H. Rules for Security Standards and Electronic Signature Standard

1. Health Plans

a. In § 142.306(a), we would require health plans to accept and apply the security standard to all health care information pertaining to an individual that is electronically maintained or electronically transmitted. Federal agencies and States may place additional requirements on their health plans. In addition, trading partners may mutually agree to implement additional security measures.

b. In § 142.310(a), entities would not be required to use an electronic signature. However, if a plan elects to use an electronic signature in one of the transactions named in the law, it would be required to apply the electronic signature standard described in § 142.310(b) to that transaction. In the future, we anticipate that the standards for other transactions may include requirements for signatures. In particular, the proposed standard for claims attachments, which will be issued in a separate regulations package later, may include signature requirements on some or all of the attachments. If the proposed attachments standard includes such signature requirements, we will address the issue of how to reconcile such requirements with existing State and Federal requirements for written signatures as part of the proposed rule.

2. Health Care Clearinghouses

a. We would require in § 142.306(b) that each health care clearinghouse comply with the security standard to ensure all health care information and activities are protected from unauthorized access. If the clearinghouse is part of a larger organization, then security must be imposed to prevent unauthorized access by the larger organization. The security standards apply to all health information pertaining to an individual that is electronically maintained or electronically transmitted.

b. In § 142.310(a), entities would not be required to use an electronic signature. However, if a plan elects to use an electronic signature in one of the transactions named in the law, it would be required to apply the electronic signature standard described in § 142.310(b) to that transaction. In the future, we anticipate that the standards for other transactions may include requirements for signatures. In particular, the proposed standard for claims attachments, which will be issued in a separate regulations package later, may include signature requirements on some or all of the attachments. If the proposed attachments standard includes such signature requirements, we will address the issue of how to reconcile such requirements with existing State and Federal requirements for written signatures as part of the proposed rule.

3. Health Care Providers

a. In § 142.306(a), we would require each health care provider to apply the security standard to all health information pertaining to an individual that is electronically maintained or electronically transmitted.

b. In § 142.310(a), entities would not be required to use an electronic signature. However, if a plan elects to use an electronic signature in one of the transactions named in the law, it would be required to apply the electronic signature standard described in § 142.310(b) to that transaction. In the future, we anticipate that the standards for other transactions may include requirements for signatures. In particular, the proposed standard for claims attachments, which will be issued in a separate regulations package later, may include signature requirements on some or all of the attachments. If the proposed attachments standard includes such signature requirements, we will address the issue of how to reconcile such requirements with existing State and Federal requirements for written signatures as part of the proposed rule.

I. Effective Dates

Health plans would be required to comply with the security and electronic signature standards as follows:

1. Each health plan that is not a small health plan would have to comply with the requirements of §§ 142.306, 142.308, and 142.310 no later than 24 months after publication of the final rule.

2. Each small health plan would have to comply with the requirements of §§ 142.306, 142.308, and 142.310 no later than 36 months after the date of publication of the final rule.

3. If the effective date for the electronic transaction standards is later than the effective date for the security standard, implementation of the security standard would not be delayed until the standard transactions are in use. The security standard would still be effective with respect to electronically stored or maintained data. Security of health information would not be solely tied to the standard transactions but would apply to all individual health information electronically stored, maintained, or transmitted.

4. Under this proposed rule, in some cases, a health plan could choose to convert from paper to standard EDI transactions prior to the effective date of the security standard. We would recommend that the security standard be implemented at that time in order to safeguard the data in those transactions. We invite comments on this issue.

Failure to comply with standards may result in monetary penalties. The Secretary is required by statute to impose penalties of not more than $100 per violation on any person who fails to comply with a standard, except that the total amount imposed on any one person in each calendar year may not exceed $25,000 for violations of one requirement.

We are not proposing any enforcement procedures at this time, but we plan to do so in a future **Federal Register** document once the industry has some experience with using the standards. These procedures will be in place by the time the standards are implemented by industry. We envision the monitoring and enforcement process as a partnership between the Federal government and the private sector. Some private accreditation bodies have already exhibited interest in certifying compliance with the security requirements as part of their accreditation reviews. Small providers may be able to self-certify through industry-developed checklists. HHS would likely retain the final responsibility for determining violations and imposing the penalties specified by the statute. We welcome comments on this approach.

III. Implementation

If an entity elects to use an electronic signature in a transaction, or if an electronic signature is required by a transaction standard adopted by the Secretary, the entity must apply the electronic signature standard described in § 142.310(b).

How the security standard would be implemented is dependent upon industry trading partner agreements for electronic transmissions. The health care industry would be able to adapt the security matrix to meet its business needs. We propose that the requirements of the security standard be implemented over time. However, we would require implementation to be complete by the applicable effective date. We would encourage, but not require that entities comply with the security standard as soon as practicable, preferably before implementing the transactions standards.

The security standard would supersede contrary provisions of State law including State law requiring medical or health plan records to be maintained or transmitted in other electronic formats. There are certain exceptions when the standards would not supersede contrary provisions of State law; section 1178 identifies those conditions and directs the Secretary to determine whether a particular State provision falls within one or more of the exceptions.

The electronic signature standard (digital signature) would be deemed to satisfy Federal and State statutory requirements for written signatures with respect to the named transactions referred to in the legislation.

Several accreditation organizations such as the Electronic Healthcare Network Accreditation Commission (EHNAC), the Joint Commission on Accreditation of Healthcare Organizations (JCAHO), and the National Committee for Quality Assurance (NCQA), indicate that one of their accreditation requirements will be compliance with the HIPAA security and electronic signature (if applicable) standards.

IV. New and Revised Standards

To encourage innovation and promote development, we plan to establish a process to allow an organization to request a revision or replacement to any adopted standard or standards. An organization could request a revision or replacement to an adopted standard by requesting a waiver from the Secretary of Health and Human Services to test a revised or new standard. The organization would be required, at a minimum, to demonstrate that the revised or new standard offers a clear improvement over the adopted standard. If the organization presents sufficient documentation that supports testing of a revised or new standard, we want to be able to grant the organization a temporary waiver to test while remaining in compliance with the law. We do not intend to establish a process that would allow an organization to avoid using any adopted standard.

We would welcome comments on the following: (1) How we should establish this process, (2) the length of time a proposed standard should be tested before we decide whether to adopt it, (3) whether we should solicit public comments before implementing a change in a standard, and (4) other issues and recommendations we should consider. Comments should be submitted to the addresses presented in the **ADDRESSES** section of this document.

The following is one possible process:

- Any organization that wishes to revise or replace an adopted standard would submit its waiver request to an HHS evaluation committee (to be established or defined). The organization would do the following for each standard it wishes to revise or replace:

+ Provide a detailed explanation, no more than 10 pages, of how the revision or replacement would be a clear improvement over the current standard.

+ Provide specifications and technical capabilities on the revised or new standard, including any additional system requirements.

+ Provide an explanation, no more than five pages, of how the organization intends to test the standard.

- The committee's evaluation would, at a minimum, be based on the following:

+ A cost-benefit analysis.

+ An assessment of whether the proposed revision or replacement demonstrates a clear improvement to an existing standard.

+ The extent and length of time of the waiver.

- The evaluation committee would inform the organization requesting the waiver within 30 working days of the committee's decision on the waiver request. If the committee decides to grant a waiver, the notification may include the following:

+ Committee comments such as the following:

—The length of time for which the waiver applies if it differs from the waiver request.

—The sites the committee believes are appropriate for testing if they differ from the waiver request.

—Any pertinent information regarding the conditions of an approved waiver.

- Any organization that receives a waiver would be required to submit a report containing the results of the study, no later than 3 months after the study is completed.

- The committee would evaluate the report and determine whether the benefits of the proposed revision or new standard significantly outweigh the disadvantages of implementing it and make a recommendation to the Secretary.

V. Response to Comments

Because of the large number of items of correspondence we normally receive on **Federal Register** documents published for comment, we are not able to acknowledge or respond to them individually. We will consider all comments we receive by the date and time specified in the **DATES** section of this preamble, and, if we proceed with a subsequent document, we will respond to the major comments in the preamble of that document.

VI. Impact Analysis

As the effect of any one standard is affected by the implementation of other standards, it can be misleading to discuss the impact of one standard by itself. Therefore, we did an impact

analysis on the total effect of all the standards in the proposed rule concerning the national provider identifier (HCFA–0045–P), which was published on May 7, 1998 (63 FR 25320).

We intend to publish in each proposed rule an impact analysis that is specific to the standard or standards proposed in that rule, but the impact analysis will assess only the relative cost impact of implementing a given standard. Thus, the following discussion contains the impact analysis for the security standard and the electronic signature standard proposed in this rule. As stated in the general impact analysis in HCFA–0045–P, we do not intend to associate costs and savings to specific standards.

Although we cannot determine the specific economic impact of the standards being proposed in this 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. Also, while each standard may not have a significant impact on a substantial number of small entities, the combined effects of all the proposed standards may have a significant effect on a substantial number of small entities. Therefore, the following impact analysis should be read in conjunction with the overall impact analysis.

The following describes the specific impacts that relate to the security and electronic signature standards. Security protection for health care information is not a ''stand-alone'' type requirement. Appropriate security protections will be a business enabler, encouraging the growth and use of electronic data interchange. The synergistic effect of the employment of the recommended security practices, procedures and technologies will enhance all aspects of HIPAA's Administrative Simplification requirements. In addition, it is important to recognize that security is not a product, but is an on-going, dynamic process.

In accordance with the provisions of Executive Order 12866, this proposed rule was reviewed by the Office of Management and Budget.

A. Security Standard

HIPAA requires that all health plans, health care providers, and health care clearinghouses that maintain or transmit health information electronically establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure integrity, confidentiality, and availability of the information. The safeguards also protect the information against any reasonably anticipated threats or hazards to the security or integrity of the information and protect it against unauthorized use or disclosure. Recommendation 1 from the National Research Council's (NRC) report *For the Record: Protecting Electronic Health Information* (''All organizations that handle patient-identifiable health care information—regardless of size—should adopt the set of technical and organization policies, practices, and procedures described * * * to protect such information.'') would apply to all health care providers regardless of size, health care clearinghouses, and health plans. We agree with the NRC's belief that implementation of the practices and technologies delineated in Recommendation 1 would be possible today, and at a reasonable cost.

Health care providers that conduct electronic transactions with health plans would have to comply with the recommendation(s) for security protection. There is, however, no requirement to maintain health records electronically or transmit health care information by electronic means. There may also be health care providers that currently submit health care information on paper but archive records electronically. These entities will need to ensure that their existing electronic systems conform to security requirements for maintaining health information. Once they have done so, however, they may also take advantage of all the other benefits of electronic recordkeeping and transmittal. Therefore, no individual small entity is expected to experience direct costs that exceed benefits as a result of this rule. Furthermore, because almost all of the NRC recommendations reflect contemporary security measures and controls, most organizations that currently have security measures should have to make few, if any, modifications to their systems to meet the requirements proposed in the security standard.

The singular exception to the above lies in the area of providing security for the electronic transmission of health care information over insecure, public media. Here, the choice of a method to use is driven by economic factors. If an organization wishes to use an insecure transmission media such as the Internet, and take advantage of the low costs involved, off-setting costs may need to be incurred to provide for an acceptable form of encryption so that health information will be protected from intercept and possible misuse.

One alternative course of action to encrypting the information would be to use the services of a VAN. VANs do not manipulate data, but rather transmit data in its native form over telecommunication lines. We anticipate that VANs would be positively affected by administrative simplification, because use of the proposed transactions standards would eliminate the need for data to be reformatted. This would allow providers to purchase the services of a VAN directly, rather than as a service bundled with the functions of other clearinghouses. Another course of action might be to use private lines which would provide an appropriate level of protection for data in transmission.

B. Electronic Signature Standard

HIPAA does not require the use of electronic signatures. This particular capability, however, would be necessary for a completely paperless environment. Certain features of the digital signature type of electronic signature make this particular system the most desirable. Only digital signatures, using current technology, provide the combination of authenticity, message integrity, and nonrepudiation which is viewed as a desirable complement to the security standards required by the law.

The use of digital signatures requires a certain infrastructure (Public Key Infrastructure) that may necessitate the expenditure of initial and recurring costs for users. We do not know what these costs are presently, due to the lack of maturity of digital signature technology, and minimal use in the marketplace today. It is noted that public key certificate management systems and services do exist today, and it is presumed more quantifiable information will be forthcoming, as to potential costs and savings that can be associated with the use of digital signature systems. Other forms of electronic signature were considered, such as biometric and digitized signatures. While they provide a useful capability in certain circumstances, we believe that digital signature technology is most appropriate for this particular application.

C. 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 EO 12866 of September 30, 1993. In order to be designated as a standard, EO 12866 requires that a proposed standard:

- Improve the efficiency and effectiveness of the health care system by leading to cost reductions for or improvements in benefits from electronic HIPAA 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 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 HIPAA 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 (such as 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, guidelines and electronic signature standards against the principles listed above, with the overall goal of achieving the maximum benefit for the least cost. We found that there exists no single standard for security or electronic signature that encompasses all the requirements that have been deemed necessary. However, in this particular area, technology is rapidly developing enhancements and better means for accomplishing the stated goals.

D. Affected Entities

1. Health Care Providers

Health care providers that conduct business using electronic transactions with other health care participants (such as other health care providers, health plans, and employers) or maintain electronic health information are encouraged, but are not required to simultaneously implement the proposed security standard. However, if the effective date for the electronic transaction standards is later than the effective date for the security standard, the implementation of the security standard will not be delayed until the standard transactions are in use.

Health care providers that transmit, receive, or maintain health information would incur implementation costs for establishing or updating their security systems. Any negative impact on these health care providers caused by implementing the proposed security standard would generally be related to the initial implementation period for the specific requirements of the security standard. Health care providers that are indirectly involved in electronic transactions (for example, those who submit a paper claim that the health plan transmits electronically to a secondary payer) and do not maintain electronic health information would not be affected.

2. Health Plans

Health plans that engage in electronic health care transactions would have to modify their systems to use the security standard and the electronic signature standard, if used. Health plans that maintain electronic health information would also have to modify their systems to use the security standard. 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 standard and other standards in a way that best fits their needs, as long as they meet the deadlines specified in the law.

Implementation of the security standard and the electronic signature standard, if used by the entities, would enhance payment safeguard activities and protect the integrity of the Medicare trust fund by reducing fraud and abuse that occurs when health care information is used by those who are not authorized to receive it. In addition these standards would assist the plans, providers, and clearinghouses to more effectively maintain the security of all health information in their databases.

3. Clearinghouses

Health care clearinghouses would face impacts similar to those experienced by health care providers and health plans. Systems vendors, that provide computer software applications to health care providers and other billers of health care services, would likely be positively affected. These vendors would have to develop software solutions that would allow health care providers and other billers of health care transactions to protect the information in their databases from unwanted access to their systems.

4. Unfunded Mandates

This proposed rule has been reviewed in accordance with the Unfunded Mandates Reform Act of 1995 (UMRA) (U.S.C. 1501 *et seq.*) and Executive Order 12875. As discussed in the combined impact analysis referenced above (see **Federal Register**, Volume 63, No. 88), DHHS estimates that implementation of the standards will require the expenditure of more than $100 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). DHHS has included this statement to address the anticipated effects of the proposed rules pursuant to section 202.

These standards also apply to State and local governments in their roles as health plans or health care providers. Thus, the proposed rules impose unfunded mandates on these entities. While we do not have sufficient information to provide estimates of these impacts, several State Medicaid agencies have estimated that it would cost $1 million per State to implement

all of the HIPAA standards. However, the Congressional Budget Office analysis stated that ''States are already in the forefront in administering the Medicaid program electronically; the only costs—which should not be significant—would involve bringing the software and computer systems for the Medicaid programs into compliance with the new standards.''

The anticipated benefits and costs of this proposed standard, and other issues raised in section 202 of the UMRA, are addressed in the analysis below, and in the combined impact analysis. In addition, 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 and in the following analysis, the Department has concluded that the rule is the most cost-effective alternative for implementation of DHHS'' statutory objective of administrative simplification.

5. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA) of 1980, Public Law 96-354, requires us to prepare a regulatory flexibility analysis if the Secretary certifies that a proposed regulation would have a significant economic impact on a substantial number of small entities. The security and electronic signature standards will affect small entities, such as providers. A more detailed analysis of the impact on small entities is part of the impact analysis we published on May 7, 1998 (63 FR 25320) for all the HIPAA standards. A detailed illustration of the potential impact of the security standard on a small health care provider can be found in the preamble in section D.

E. Factors in Establishing the Security Standard

1. Selection of Security Systems and Procedures

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 conform to the new standard. Implementation of the security standard would require all health plans, health care providers, and health care clearinghouses to establish or revise their security precautions because the proposed standard is not currently in use. The selection of the security standard does not impose a greater burden on the industry than the nonselected options, and presents significant advantages in terms of universality, uniqueness and flexibility.

Only those plans, providers, and clearinghouses that decide to use the digital signature would be affected by the electronic signature standard. Some large health plans, health care providers, and health care clearinghouses that currently exchange health information among trading partners may have security systems and procedures in place to protect the information from unauthorized access. These entities may not incur significant costs to meet the proposed security standard and if they opt not to use the digital signature they would not incur costs to meet the electronic signature requirements. Also, some entities that currently use electronic signatures as an added security measure may also be using digital signature technology. At most, large entities that may have sophisticated security systems in place may only need to revise or update their systems to meet the proposed security standard and electronic signature standard.

2. Complexity of Conversion

The complexity of the conversion would be significantly affected by the volume of claims health plans process electronically and the desire to transmit the claims themselves or to use the services of a VAN or a clearinghouse. If they chose to transmit themselves, they would need to convert to the proposed transaction standards. Specific technology limitations of existing systems could affect the complexity of the conversion. For example, some entities may only have a minimum level of security and procedures in place and therefore may require a full upgrade, while others may already have a very sophisticated system and procedures and require very little enhancement.

3. Cost of Conversion

We expect that most providers, health plans, and clearinghouses that transmit or store data electronically have already implemented some security measures and will primarily need to assess existing security, identify areas of risk, and implement additional measures. 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 (*e.g.*, 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 utilize 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 or software purchases at the time they do routine equipment upgrades.

The security requirements we are proposing were developed with considerable input from the health care industry, including providers, health plans, clearinghouses, vendors, and standards organizations. Industry members strongly advocated this flexible approach, which permits each affected entity to develop cost-effective security measures. We believe that this approach will yield the lowest implementation cost to industry while assuring that health information is safeguarded. We solicit input regarding implementation costs.

We are unable to estimate, of the nation's 4 million-plus health plans and 1.2 million-plus providers, the number of entities that would require security systems and procedures because they conduct electronic transactions or maintain electronic health information. Nor are we able to estimate the number of entities that neither conduct electronic transactions nor maintain electronic health information 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 because they would have no need to implement security standards.) However, we are aware of the possibility that those small entities that currently process claims electronically or maintain electronic health information may not be able to continue to do so due to the cost of establishing security systems to meet the requirements of the proposed security standard. Those entities that are not able to bill and exchange health information electronically may use clearinghouses. We believe that the proposed security standard represents the minimum necessary for adequate protection of health information in an electronic format. 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, we are also unable to estimate the cost to the entities that will process electronic transactions.

However, we believe that the cost of establishing security systems and procedures is a portion of the costs associated with converting to the transaction standards that are required under HIPAA.

This discussion on conversion costs relates only to health plans, health care providers, and health care clearinghouses that are required to follow the security standard to maintain, transmit or receive electronic health information. Other entities would not be required to follow the security standard and procedures until they choose to maintain, transmit, or receive electronic health information. The cost of establishing security systems and procedures for entities that do not transmit, receive or maintain health information electronically is not included in our estimates.

VII. Collection of Information Requirements

Under the Paperwork Reduction Act of 1995, we are required to provide 60-day notice in the **Federal Register** and solicit public comment before a collection of information requirement is submitted to the Office of Management and Budget (OMB) for review and approval. In order to fairly evaluate whether an information collection should be approved by OMB, section 3506(c)(2)(A) of the Paperwork Reduction Act of 1995 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 § 142.308 of this document. In addition, we are soliciting comment on the applicability of the PRA as it may relate to the requirement to use the standard adopted in § 142.310 of this regulation.

Section 142.308 Security Standard

In summary, each entity designated in § 142.302 must maintain documentation demonstrating the development, implementation, and maintenance of appropriate security measures that include, at a minimum, the requirements and implementation features set forth in this section. In addition, entities must maintain necessary documentation to demonstrate that these measures have been periodically reviewed, validated, updated, and kept current.

While we solicit comment on these recordkeeping requirements we explicitly solicit comment on the burden associated with maintaining documentation related to the implementation the requirements set forth in § 142.308. Since the level of documentation necessary to demonstrate compliance with these requirements is dependent upon individual business needs and the fact that we do not prescribe the form, format, or degree of documentation necessary to demonstrate compliance, we are currently unable to accurately estimate the degree of recordkeeping burden that will be experienced by the varying entities. Therefore, commentors should provide an estimate of: (1) the initial recordkeeping burden associated with meeting these requirements and (2) the recordkeeping burden associated with maintaining documentation to demonstrate that the measures have been periodically reviewed, validated, updated, and kept current.

Below is a discussion of the applicability of the PRA as it may relate to the adoption of the standard referenced in § 142.310 of this regulation.

Section 142.310 Electronic Signature Standard

In summary, any entity electing to use an electronic signature in a transaction as defined in § 142.103, or if an electronic signature is required by a transaction standard adopted by the Secretary, the entity must apply the electronic signature standard described in paragraph (b) of this section to that transaction.

Discussion

The emerging and increasing use of health care EDI standards and transactions raises the issue of the applicability of the PRA. The question arises whether a regulation that adopts an EDI standard used to exchange certain information constitutes an information collection subject to the PRA.

In particular, we are still considering whether the use of any EDI transaction standard, such as the electronic signature described in this regulation, should be viewed or regarded as a standardized electronic collection of information. If it is a standardized electronic information collection, then the requirement by the Federal government on the industry to accept and transmit the information may be subject to OMB review and approval under the PRA.

We invite public comment on the issues discussed above. If the requirements, as set forth in § 142.310 are determined to be subject to the PRA, we will submit these requirements to OMB for PRA approval. If you comment on these information collection and recordkeeping requirements, please e-mail comments to JBurke1@hcfa.gov (Attn: HCFA–0049) or mail copies directly to the following:

Health Care Financing Administration, Office of Information Services, Security and Standards Group, Division of HCFA Enterprise Standards, Room N2–14–26, 7500 Security Boulevard, Baltimore, MD 21244–1850. Attn: John Burke HCFA–0049, HCFA Reports Clearance Officer

And

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

List of Subjects in 45 CFR Part 142

Administrative practice and procedure, Health facilities, Health insurance, Hospitals, Medicaid, Medicare, Report and recordkeeping requirement.

45 CFR subtitle A, subchapter B, would be amended by adding part 42 to read as follows:

Note to Reader: This proposed rule is one of several proposed rules that are being published to implement the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996. We propose to establish a new 45 CFR Part 142. Proposed Subpart A—General Provisions is exactly the same in each rule unless we have added new sections or definitions to incorporate additional general information. The subparts that follow relate to the specific provisions announced separately in each proposed rule. When we publish the first final rule, each subsequent final rule will revise or add to the text that is set out in the first final rule.

PART 142—ADMINISTRATIVE REQUIREMENTS

Subpart A—General Provisions

Sec.

Subpart B—Reserved

Subpart C—Security and Electronic Signature Standards

Authority: Sections 1173 and 1175 of the Social Security Act (42 U.S.C. 1320d–2 and 1320d–4).

Subpart A—General Provisions

§ 142.101 Statutory basis and purpose.

Sections 1171 through 1179 of the Social Security Act, 42 U.S.C. 1320d, as added by section 262 of the Health Insurance Portability and Accountability Act of 1996, require HHS to adopt national standards for the electronic exchange of health information in the health care system. The purpose of the sections of this part is to promote administrative simplification.

§ 142.102 Applicability.

(a) The standards adopted or designated under this part apply, in whole or in part, to the following:

(1) A health plan.

(2) A health care clearinghouse when doing the following:

(i) Transmitting a standard transaction (as defined in § 142.103) to a health care provider or health plan.

(ii) Receiving a standard transaction from a health care provider or health plan.

(iii) Transmitting and receiving the standard transactions when interacting with another health care clearinghouse.

(3) A health care provider when transmitting an electronic transaction as defined in § 142.103.

(b) Means of compliance are stated in greater detail in § 142.105.

§ 142.103 Definitions.

For purposes of this part, the following definitions apply:

Code set means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

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

Health care provider means a provider of services as defined in section 1861(u) of the Social Security Act, 42 U.S.C. 1395x, a provider of medical or other health services as defined in section 1861(s) of the Social Security Act, and any other person who furnishes or bills and is paid for health care services or supplies in the normal course of business.

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

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

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

Health plan means an individual or group plan that provides, or pays the cost of, medical care. Health plan includes the following, singly or in combination:

(1) Group health plan. A group health plan is an employee welfare benefit plan (as currently defined in section 3(1) of the Employee Retirement Income and Security Act of 1974, 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, or otherwise, and—

(i) Has 50 or more participants; or

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Medical care means the diagnosis, cure, mitigation, treatment, or prevention of disease, or amounts paid for the purpose of affecting any body structure or function of the body; amounts paid for transportation primarily for and essential to these items; and amounts paid for insurance covering the items and the transportation specified in this definition.

Participant means any employee or former employee of an employer, or any member or former member of an employee organization, who is or may become eligible to receive a benefit of any type from an employee benefit plan that covers employees of that employer or members of such an organization, or whose beneficiaries may be eligible to receive any of these benefits. ''Employee'' includes an individual who is treated as an employee under section 401(c)(1) of the Internal Revenue Code of 1986 (26 U.S.C. 401(c)(1)).

Small health plan means a group health plan or individual health plan with fewer than 50 participants.

Standard means a set of rules for a set of codes, data elements, transactions, or identifiers promulgated either by an organization accredited by the American National Standards Institute or HHS for the electronic transmission of health information.

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

(1) Health claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health claims status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

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

§ 142.104 General requirements for health plans.

If a person conducts a transaction (as defined in § 142.103) with a health plan as a standard transaction, the following apply:

(a) The health plan may not refuse to conduct the transaction as a standard transaction.

(b) The health plan may not delay the transaction or otherwise adversely affect, or attempt to adversely affect, the person or the transaction on the ground that the transaction is a standard transaction.

(c) The health information transmitted and received in connection with the transaction must be in the form of standard data elements of health information.

(d) A health plan that conducts transactions through an agent must assure that the agent meets all the requirements of this part that apply to the health plan.

§ 142.105 Compliance using a health care clearinghouse.

(a) Any person or other entity subject to the requirements of this part may meet the requirements to accept and transmit standard transactions by either—

(1) Transmitting and receiving standard data elements; or

(2) Submitting nonstandard data elements to a health care clearinghouse for processing into standard data elements and transmission by the health care clearinghouse and receiving standard data elements through the health care clearinghouse.

(b) The transmission, under contract, of nonstandard data elements between a health plan or a health care provider and its agent health care clearinghouse is not a violation of the requirements of this part.

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

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

Subpart B—[Reserved]

Subpart C—Security and Electronic Signature Standards

§ 142.302 Applicability and scope.

The standards adopted or designated under this subpart apply, in whole or in part, to the following:

(a) A health plan.

(b) A health care clearinghouse or health care provider that takes one of the following actions:

(1) Processes any electronic transmission between any combination of health care entities listed in this section.

(2) Electronically maintains any health information used in an electronic transmission that has been sent or received between any combination of health care entities listed in this section.

§ 142.304 Definitions.

For purposes of this subpart, the following definitions apply:

Access refers to the ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.

Access control refers to 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, and classification.

Authentication refers to the corroboration that an entity is the one claimed.

Contingency plan refers to a plan for responding to a system emergency. The plan includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster.

Encryption (or encipherment) refers to transforming confidential plaintext into ciphertext to protect it. An encryption algorithm combines plaintext with other values called keys, or ciphers, so the data becomes unintelligible. Once encrypted, data can be stored or transmitted over unsecured lines. Decrypting data reverses the encryption algorithm process and makes the plaintext available for further processing.

Password refers to confidential authentication information composed of a string of characters.

Role-based access control (RBAC) is an alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. With RBAC, rather than attempting to map an organization's security policy to a relatively low-level set of technical controls (typically, access control lists), each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

Token refers to a physical item necessary for user identification when used in the context of authentication. For example, an electronic device that can be inserted in a door or a computer system to obtain access.

User-based access refers to a security mechanism used to grant users of a system access based upon the identity of the user.

§ 142.306 Rules for the security standard.

(a) An entity must apply the security standard described in § 142.308 to all health information pertaining to an individual that is electronically maintained or electronically transmitted.

(b) If a health care clearinghouse is part of a larger organization, it must assure that all health information pertaining to an individual is protected from unauthorized access by the larger organization.

§ 142.308 Security standard.

Each entity designated in § 142.302 must assess potential risks and vulnerabilities to the individual health data in its possession and develop, implement, and maintain appropriate security measures. These measures must be documented and kept current, and must include, at a minimum, the following requirements and implementation features:

(a) *Administrative procedures to guard data integrity, confidentiality, and availability* (documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data). These procedures include the following requirements:

(1) Certification. (The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external accrediting agency.)

(2) A chain of trust partner agreement (a contract entered into by two business partners in which the partners agree to electronically exchange data and protect the integrity and confidentiality of the data exchanged).

(3) A contingency plan, a routinely updated plan for responding to a system emergency, that includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster. The plan must include all of the following implementation features:

(i) An applications and data criticality analysis (an entity's formal assessment of the sensitivity, vulnerabilities, and security of its programs and information it receives, manipulates, stores, and/or transmits).

(ii) Data backup plan (a documented and routinely updated plan to create and maintain, for a specific period of time, retrievable exact copies of information).

(iii) A disaster recovery plan (the part of an overall contingency plan that contains a process enabling an enterprise to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure).

(iv) Emergency mode operation plan (the part of an overall contingency plan that contains a process enabling an enterprise to continue to operate in the event of fire, vandalism, natural disaster, or system failure).

(v) Testing and revision procedures (the documented process of periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary).

(4) Formal mechanism for processing records (documented policies and procedures for the routine, and nonroutine, receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information).

(5) Information access control (formal, documented policies and procedures for granting different levels of access to health care information) that includes all of the following implementation features:

(i) Access authorization (information-use policies and procedures that establish the rules for granting access, (for example, to a terminal, transaction, program, process, or some other user.)

(ii) Access establishment (security policies and rules that determine an entity's initial right of access to a terminal, transaction, program, process or some other user).

(iii) Access modification (security policies and rules that determine the types of, and reasons for, modification to an entity's established right of access, to a terminal, transaction, program, process, or some other user.)

(6) Internal audit (in-house review of the records of system activity (such as logins, file accesses, and security incidents) maintained by an organization).

(7) Personnel security (all personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances) that includes all of the following implementation features:

(i) Assuring supervision of maintenance personnel by an authorized, knowledgeable person. These procedures are documented formal procedures and instructions for the oversight of maintenance personnel when the personnel are near health information pertaining to an individual.

(ii) Maintaining a record of access authorizations (ongoing documentation and review of the levels of access granted to a user, program, or procedure accessing health information).

(iii) Assuring that operating and maintenance personnel have proper access authorization (formal documented policies and procedures for determining the access level to be granted to individuals working on, or near, health information).

(iv) Establishing personnel clearance procedures (a protective measure applied to determine that an individual's access to sensitive unclassified automated information is admissible).

(v) Establishing and maintaining personnel security policies and procedures (formal, documentation of procedures to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances).

(vi) Assuring that system users, including maintenance personnel, receive security awareness training.

(8) Security configuration management (measures, practices, and procedures for the security of information systems that must be coordinated and integrated with each other and other measures, practices, and procedures of the organization established in order to create a coherent system of security) that includes all of the following implementation features:

(i) Documentation (written security plans, rules, procedures, and instructions concerning all components of an entity's security).

(ii) Hardware and software installation and maintenance review and testing for security features (formal, documented procedures for connecting and loading new equipment and programs, periodic review of the maintenance occurring on that equipment and programs, and periodic security testing of the security attributes of that hardware/software).

(iii) Inventory (the formal, documented identification of hardware and software assets).

(iv) Security testing (process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed applications environment; this process includes hands-on functional testing, penetration testing, and verification).

(v) Virus checking. (The act of running a computer program that identifies and disables:

(A) Another ''virus'' computer program, typically hidden, that attaches itself to other programs and has the ability to replicate.

(B) A code fragment (not an independent program) that reproduces by attaching to another program.

(C) A code embedded within a program that causes a copy of itself to be inserted in one or more other programs.)

(9) Security incident procedures (formal documented instructions for reporting security breaches) that include all of the following implementation features:

(i) Report procedures (documented formal mechanism employed to document security incidents).

(ii) Response procedures (documented formal rules or instructions for actions to be taken as a result of the receipt of a security incident report).

(10) Security management process (creation, administration, and oversight of policies to ensure the prevention, detection, containment, and correction of security breaches involving risk analysis and risk management). It includes the establishment of accountability, management controls (policies and education), electronic controls, physical security, and penalties for the abuse and misuse of its assets (both physical and electronic) that includes all of the following implementation features:

(i) Risk analysis, a process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.

(ii) Risk management (process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk).

(iii) Sanction policies and procedures (statements regarding disciplinary actions that are communicated to all employees, agents, and contractors; for example, verbal warning, notice of disciplinary action placed in personnel files, removal of system privileges, termination of employment, and contract penalties). They must include employee, agent, and contractor notice of civil or criminal penalties for misuse or misappropriation of health information and must make employees, agents, and contractors aware that violations may result in notification to law enforcement officials and regulatory, accreditation, and licensure organizations.

(iv) Security policy (statement(s) of information values, protection responsibilities, and organization commitment for a system). This is the framework within which an entity establishes needed levels of information security to achieve the desired confidentiality goals.

(11) Termination procedures (formal documented instructions, which include appropriate security measures, for the ending of an employee's employment or an internal/external user's access) that include procedures for all of the following implementation features:

(i) Changing locks (a documented procedure for changing combinations of locking mechanisms, both on a recurring basis and when personnel knowledgeable of combinations no longer have a need to know or require access to the protected facility or system).

(ii) Removal from access lists (physical eradication of an entity's access privileges).

(iii) Removal of user account(s) (termination or deletion of an individual's access privileges to the information, services, and resources for which they currently have clearance, authorization, and need-to-know when such clearance, authorization and need-to-know no longer exists).

(iv) Turning in of keys, tokens, or cards that allow access (formal, documented procedure to ensure all physical items that allow a terminated employee to access a property, building, or equipment are retrieved from that employee, preferably before termination).

(12) Training (education concerning the vulnerabilities of the health information in an entity's possession and ways to ensure the protection of that information) that includes all of the following implementation features:

(i) Awareness training for all personnel, including management personnel (in security awareness, including, but not limited to, password maintenance, incident reporting, and viruses and other forms of malicious software).

(ii) Periodic security reminders (employees, agents, and contractors are made aware of security concerns on an ongoing basis).

(iii) User education concerning virus protection (training relative to user awareness of the potential harm that can be caused by a virus, how to prevent the introduction of a virus to a computer system, and what to do if a virus is detected).

(iv) User education in importance of monitoring log-in success or failure and how to report discrepancies (training in the user's responsibility to ensure the security of health care information).

(v) User education in password management (type of user training in the rules to be followed in creating and changing passwords and the need to keep them confidential).

(b) *Physical safeguards to guard data integrity, confidentiality, and availability.* Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. It covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities. Physical safeguards must include all of the following requirements and implementation features:

(1) Assigned security responsibility (practices established by management to manage and supervise the execution and use of security measures to protect data and to manage and supervise the conduct of personnel in relation to the protection of data).

(2) Media controls (formal, documented policies and procedures that govern the receipt and removal of hardware/software (such as diskettes and tapes) into and out of a facility) that include all of the following implementation features:

(i) Access control.

(ii) Accountability (the property that ensures that the actions of an entity can be traced uniquely to that entity).

(iii) Data backup (a retrievable, exact copy of information).

(iv) Data storage (the retention of health care information pertaining to an individual in an electronic format).

(v) Disposal (final disposition of electronic data, and/or the hardware on which electronic data is stored).

(3) Physical access controls (limited access) (formal, documented policies and procedures to be followed to limit physical access to an entity while ensuring that properly authorized access is allowed) that include all of the following implementation features:

(i) Disaster recovery (the process enabling an entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure).

(ii) An emergency mode operation (access controls in place that enable an entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure).

(iii) Equipment control (into and out of site) (documented security procedures for bringing hardware and software into and out of a facility and for maintaining a record of that equipment. This includes, but is not limited to, the marking, handling, and disposal of hardware and storage media.)

(iv) A facility security plan (a plan to safeguard the premises and building (exterior and interior) from unauthorized physical access and to safeguard the equipment therein from unauthorized physical access, tampering, and theft).

(v) Procedures for verifying access authorizations before granting physical access (formal, documented policies and instructions for validating the access privileges of an entity before granting those privileges).

(vi) Maintenance records (documentation of repairs and modifications to the physical components of a facility, such as

hardware, software, walls, doors, and locks).

(vii) Need-to-know procedures for personnel access (a security principle stating that a user should have access only to the data he or she needs to perform a particular function).

(viii) Procedures to sign in visitors and provide escorts, if appropriate (formal documented procedure governing the reception and hosting of visitors).

(ix) Testing and revision (the restriction of program testing and revision to formally authorized personnel).

(4) Policy and guidelines on work station use (documented instructions/ procedures delineating 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 computer terminal site or type of site, dependent upon the sensitivity of the information accessed from that site).

(5) A secure work station location (physical safeguards to eliminate or minimize the possibility of unauthorized access to information; for example, locating a terminal used to access sensitive information in a locked room and restricting access to that room to authorized personnel, not placing a terminal used to access patient information in any area of a doctor's office where the screen contents can be viewed from the reception area).

(6) Security awareness training (information security awareness training programs in which all employees, agents, and contractors must participate, including, based on job responsibilities, customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security).

(c) *Technical security services to guard data integrity, confidentiality, and availability* (the processes that are put in place to protect information and to control individual access to information). These services include the following requirements and implementation features:

(1) The technical security services must include all of the following requirements and the specified implementation features:

(i) Access control that includes:

(A) A procedure for emergency access (documented instructions for obtaining necessary information during a crisis), and

(B) At least one of the following implementation features:

(*1*) Context-based access (an access control procedure based on the context of a transaction (as opposed to being based on attributes of the initiator or target)).

(*2*) Role-based access.

(*3*) User-based access.

(C) The optional use of encryption.

(ii) Audit controls (mechanisms employed to record and examine system activity).

(iii) Authorization control (the mechanism for obtaining consent for the use and disclosure of health information) that includes at least one of the following implementation features:

(A) Role-based access.

(B) User-based access.

(iv) Data authentication. (The corroboration that data has not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, double keying, a message authentication code, or digital signature.)

(v) Entity authentication (the corroboration that an entity is the one claimed) that includes:

(A) Automatic logoff (a security procedure that causes an electronic session to terminate after a predetermined time of inactivity, such as 15 minutes), and

(B) Unique user identifier (a combination name/number assigned and maintained in security procedures for identifying and tracking individual user identity).

(C) At least one of the following implementation features:

(*1*) Biometric identification (an identification system that identifies a human from a measurement of a physical feature or repeatable action of the individual (for example, hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand written signature)).

(*2*) Password.

(*3*) Personal identification number (PIN) (a number or code assigned to an individual and used to provide verification of identity).

(*4*) A telephone callback procedure (method of authenticating the identity of the receiver and sender of information through a series of ''questions'' and ''answers'' sent back and forth establishing the identity of each). For example, when the communicating systems exchange a series of identification codes as part of the initiation of a session to exchange information, or when a host computer disconnects the initial session before the authentication is complete, and the host calls the user back to establish a session at a predetermined telephone number.

(*5*) Token.

(2) [Reserved]

(d) *Technical security mechanisms* (processes that are put in place to guard against unauthorized access to data that is transmitted over a communications network).

(1) If an entity uses communications or network controls, its security standards for technical security mechanisms must include the following:

(i) The following implementation features:

(A) Integrity controls (a security mechanism employed to ensure the validity of the information being electronically transmitted or stored).

(B) Message authentication (ensuring, typically with a message authentication code, that a message received (usually via a network) matches the message sent).

(ii) One of the following implementation features:

(A) Access controls (protection of sensitive communications transmissions over open or private networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient).

(B) Encryption.

(2) If an entity uses network controls (to protect sensitive communication that is transmitted electronically over open networks so that it cannot be easily intercepted and interpreted by parties other than the intended recipient), its technical security mechanisms must include all of the following implementation features:

(i) Alarm. (In communication systems, any device that can sense an abnormal condition within the system and provide, either locally or remotely, a signal indicating the presence of the abnormality. The signal may be in any desired form ranging from a simple contact closure (or opening) to a time-phased automatic shutdown and restart cycle.)

(ii) Audit trail (the data collected and potentially used to facilitate a security audit).

(iii) Entity authentication (a communications or network mechanism to irrefutably identify authorized users, programs, and processes and to deny access to unauthorized users, programs, and processes).

(iv) Event reporting (a network message indicating operational irregularities in physical elements of a network or a response to the occurrence of a significant task, typically the completion of a request for information).

§ 142.310 Electronic signature standard.

(a) *General rule.* If an entity elects to use an electronic signature in a

transaction as defined in § 142.103, or if an electronic signature is required by a transaction standard adopted by the Secretary, the entity must apply the electronic signature standard described in paragraph (b) of this section to that transaction.

(b) *Standard.*

(1) An electronic signature is the attribute affixed to an electronic document to bind it to a particular entity. An electronic signature secures the user authentication (proof of claimed identity) at the time the signature is generated; creates the logical manifestation of signature (including the possibility for multiple parties to sign a document and have the order of application recognized and proven); supplies additional information such as time stamp and signature purpose specific to that user; and ensures the integrity of the signed document to enable transportability of data, interoperability, independent verifiability, and continuity of signature capability. Verifying a signature on a document verifies the integrity of the document and associated attributes and verifies the identity of the signer.

(2) The standard for electronic signature is a digital signature. A ''digital signature'' is an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters so that the identity of the signer and the integrity of the data can be verified.

(c) *Required implementation features.* If an entity uses electronic signatures, the signature method must assure all of the following features:

(1) Message integrity (the assurance of unaltered transmission and receipt of a message from the sender to the intended recipient).

(2) Nonrepudiation (strong and substantial evidence of the identity of the signer of a message, and of message integrity, sufficient to prevent a party from successfully denying the origin, submission, or delivery of the message and the integrity of its contents).

(3) User authentication (the provision of assurance of the claimed identity of an entity).

(d) *Optional implementation features.* If an entity uses electronic signatures, the entity may also use, among others, any of the following implementation features:

(1) Ability to add attributes (one possible capability of a digital signature technology; for example, the ability to add a time stamp as part of a digital signature).

(2) Continuity of signature capability (the concept that the public verification of a signature must not compromise the ability of the signer to apply additional secure signatures at a later date).

(3) Countersignatures. (The capability to prove the order of application of signatures. This is analogous to the normal business practice of countersignatures, where a party signs a document that has already been signed by another party.)

(4) Independent verifiability (the capability to verify the signature without the cooperation of the signer).

(5) Interoperability (the applications used on either side of a communication, between trading partners and/or between internal components of an entity, are able to read and correctly interpret the information communicated from one to the other).

(6) Multiple signatures. (With this feature, multiple parties are able to sign a document. Conceptually, multiple signatures are simply appended to the document.)

(7) Transportability of data (the ability of a signed document to be transported over an insecure network to another system, while maintaining the integrity of the document, including content, signatures, signature attributes, and (if present) document attributes).

§ 142.312 Effective date of the initial implementation of the security and electronic signature standards.

(a) *General rules.*

(1) Except for a small health plan (defined at § 142.103), each entity designated in § 142.302 must comply with the requirements of this subpart by [24 months after the effective date of the final rule in the **Federal Register**].

(2) A delay in an effective date for using a standard transaction described in this part does not delay the effective dates described in paragraphs (a)(1) and (b) of this section.

(3) The requirements of the security standard may be implemented over time. Implementation must be completed by the applicable effective date.

(b) *Small health plans.* A small health plan must comply with the requirements of this subpart by [36 months after the effective date of the final rule in the **Federal Register**].

Authority: Sections 1173 and 1175 of the Social Security Act (42 U.S.C. 1320d–2 and 1320d–4).

Dated: July 15, 1998.

Donna E. Shalala,

Secretary.

Note: The following appendix will not appear in the Code of Federal Regulations.

Addendum 1

HIPAA Security Matrix

Please Note: (1) While we have attempted to categorize security requirements for ease of understanding and reading clarity, there are overlapping areas on the matrix in which the same requirements are restated in a slightly different context. (2) To ensure that no Requirement or Implementation feature is considered more important than another, this matrix has been presented, within each subject area, in alphabetical order.

ADMINISTRATIVE PROCEDURES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation
Certification	
Chain of trust partner agreement	
Contingency plan (all listed implementation features must be implemented).	Applications and data criticality analysis. Data backup plan. Disaster recovery plan. Emergency mode operation plan. Testing and revision.
Formal mechanism for processing records.	
Information access control (all listed implementation features must be implemented).	Access authorization. Access establishment. Access modification.
Internal audit	

ADMINISTRATIVE PROCEDURES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY—Continued

Requirement	Implementation
Personnel security (all listed implementation features must be implemented).	Assure supervision of maintenance personnel by authorized, knowledgeable person. Maintainance of record of access authorizations. Operating, and in some cases, maintenance personnel have proper access authorization. Personnel clearance procedure. Personnel security policy/procedure. System users, including maintenance personnel, trained in security.
Security configuration mgmt. (all listed implementation features must be implemented).	Documentation. Hardware/software installation & maintenance review and testing for security features. Inventory. Security Testing. Virus checking.
Security incident procedures (all listed implementation features must be implemented).	Report procedures. Response procedures.
Security management process (all listed implementation features must be implemented).	Risk analysis. Risk management. Sanction policy. Security policy.
Termination procedures (all listed implementation features must be implemented).	Combination locks changed. Removal from access lists. Removal of user account(s). Turn in keys, token or cards that allow access.
Training (all listed implementation features must be implemented)	Awareness training for all personnel (including mgmt). Periodic security reminders. User education concerning virus protection. User education in importance of monitoring log in success/failure, and how to report discrepancies. User education in password management.

PHYSICAL SAFEGUARDS TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation
Assigned security responsibility	
Media controls (all listed implementation features must be implemented).	Access control. Accountability (tracking mechanism). Data backup. Data storage. Disposal.
Physical access controls (limited access) (all listed implementation features must be implemented).	Disaster recovery. Emergency mode operation. Equipment control (into and out of site). Facility security plan. Procedures for verifying access authorizations prior to physical access. Maintenance records. Need-to-know procedures for personnel access. Sign-in for visitors and escort, if appropriate. Testing and revision.
Policy/guideline on work station use	
Secure work station location	
Security awareness training	

TECHNICAL SECURITY SERVICES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation
Access control (The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context-based access, Roll-based access, User-based access. The use of Encryption is optional).	Context-based access. Encryption. Procedure for emergency access. Role-based access. User-based access.
Audit controls	
Authorization Control (At least one of the listed implementation features must be implemented).	Role-based access. User-based access
Data Authentication	

TECHNICAL SECURITY SERVICES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY—Continued

Requirement	Implementation
Entity Authentication (The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented).	Automatic logoff. Biometric. Password. PIN. Telephone callback. Token. Unique user identification.

TECHNICAL SECURITY MECHANISMS TO GUARD AGAINST UNAUTHORIZED ACCESS TO DATA THAT IS TRANSMITTED OVER A COMMUNICATIONS NETWORK

Requirement	Implementation
Communications/network controls (The following implementation features must be implemented: Integrity controls, Message authentication. If communications or networking is employed, one of the following implementation features must be implemented: Access controls, Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting).	Access controls. Alarm. Audit trail. Encryption. Entity authentication. Event reporting. Integrity controls. Message authentication.

ELECTRONIC SIGNATURE

Requirement	Implementation
Digital signature (If digital signature is employed, the following three implementation features must be implemented: Message integrity, Non-repudiation, User authentication. Other implementation features are optional).	Ability to add attributes. Continuity of signature capability. Counter signatures. Independent verifiability. Interoperability. Message integrity. Multiple Signatures. Non-repudiation. Transportability. User authentication.

Addendum 2—HIPAA Security and Electronic Signature Standards Glossary of Terms

Please Note:

(1) While we have attempted to categorize security requirements for ease of understanding and reading clarity, there are overlapping areas on the matrix in which the same requirements are restated in a slightly different context.

(2) While not appearing on the matrix, a number of terms listed below do appear in the glossary descriptions and have been supplied for additional clarity:

(3) The definitions provided in this document have been obtained from multiple sources.

Ability to add attributes:
- One possible capability of a digital signature technology, for example, the ability to add a time stamp as part of a digital signature.
- Part of digital signature on the matrix.

Access:
- The ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.

Access authorization:
- Information-use policies/procedures that establish the rules for granting and/or restricting access to a user, terminal, transaction, program, or process.
- Part of information access control on the matrix.

Access control:
- A method of restricting access to resources, allowing only privileged entities access. (PGP, Inc.)
- Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, classification, and subject-object separation.
- Part of Media Controls on the matrix.
- Part of technical security services to control and monitor access to information on the matrix.

Access controls:
- The protection of sensitive communications transmissions over open or private networks so that it cannot be easily intercepted and interpreted by parties other than the intended recipient.
- Part of mechanisms to prevent unauthorized access to data that is transmitted over a communications network on the matrix.

Access establishment:
- The security policies, and the rules established therein, that determine an entity's initial right of access to a terminal, transaction, program, or process.
- Part of information access control on the matrix.

Access Level:
- A level associated with an individual who may be accessing information (for example, a clearance level) or with the information which may be accessed (for example, a classification level). (NRC, 1991, as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)

Access modification:
- The security policies, and the rules established therein, that determine types of, and reasons for, modification to an entity's established right of access to a terminal, transaction, program, or process.
- Part of information access control on the matrix.

Accountability:
- The property that ensures that the actions of an entity can be traced uniquely to that entity. (ASTM E1762—95)

Part of media controls on the matrix.

Administrative procedures to guard data integrity, confidentiality and availability:
Documented, formal practices to manage (1) the selection and execution of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data.
A section of the matrix.

Alarm, event reporting, and audit trail:
(1) Alarm: In communication systems, any device that can sense an abnormal condition within the system and provide, either locally or remotely, a signal indicating the presence of the abnormality. (188) NOTE: The signal may be in any desired form ranging from a simple contact closure (or opening) to a time-phased automatic shutdown and restart cycle. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
(2) Event reporting: Network message indicating operational irregularities in physical elements of a network or a response to the occurrence of a significant task, typically the completion of a request for information. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
(3) Audit trail: Data collected and potentially used to facilitate a security audit. (ISO 7498–2, as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)
Part of mechanisms to prevent unauthorized access to data that is transmitted over a communications network on the matrix.

Applications and data criticality analysis:
An entity's formal assessment of the sensitivity, vulnerabilities, and security of its programs and information it receives, manipulates, stores, and/or transmits.
Part of contingency plan on the matrix.

Assigned security responsibility:
Practices put in place by management to manage and supervise (1) the execution and use of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data.
Part of Physical safeguards to guard data integrity, confidentiality, and availability on the matrix.

Assure supervision of maintenance personnel by authorized, knowledgeable person:
Documented formal procedures/instruction for the oversight of maintenance personnel when such personnel are in the vicinity of health information pertaining to an individual.
Part of personnel security on the matrix.

Asymmetric encryption:
Encryption and decryption performed using two different keys, one of which is referred to as the public key and one of which is referred to as the private key.
Also known as public-key encryption. (Stallings)

Asymmetric key:
One half of a key pair used in an asymmetric (''public-key'') encryption system. Asymmetric encryption systems have two important properties: (1) the key used for encryption is different from the one used for decryption (2) neither key can feasibly be derived from the other. (CORBA Security Services, 1997)

Audit controls:
The mechanisms employed to record and examine system activity.
Part of technical security services to control and monitor access to information on the matrix.

Authorization control:
The mechanism for obtaining consent for the use and disclosure of health information.
Part of technical security services to control and monitor access to information on the matrix.

Automatic logoff:
After a pre-determined time of inactivity (for example, 15 minutes), an electronic session is terminated.
Part of entity authentication on the matrix.

Availability:
The property of being accessible and useable upon demand by an authorized entity. (ISO 7498–2, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)

Awareness training for all personnel (including management):
All personnel in an organization should undergo security awareness training, including, but not limited to, password maintenance, incident reporting, and an education concerning viruses and other forms of malicious software.
Part of Training on the matrix.

Biometric:.
A biometric identification system identifies a human from a measurement of a physical feature or repeatable action of the individual (for example, hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand written signature). (ASTM E1762—95, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)
Part of entity authentication on the matrix.

Certification:
The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external accrediting agency.
Part of administrative procedures to guard data integrity, confidentiality, and availability.

Chain of Trust Partner Agreement:
Contract entered into by two business partners in which it is agreed to exchange data and that the first party will transmit information to the second party, where the data transmitted is agreed to be protected between the partners. The sender and receiver depend upon each other to maintain the integrity and confidentiality of the transmitted information. Multiple such two-party contracts may be involved in moving information from the originator to the ultimate recipient, for example, a provider may contract with a clearing house to transmit claims to the clearing house; the clearing house, in turn, may contract with another clearing house or with a payer for the further transmittal of those same claims.
Part of administrative procedures to guard data integrity, confidentiality and availability on the matrix..

Classification:
Protection of data from unauthorized access by the designation of multiple levels of access authorization clearances to be required for access, dependent upon the sensitivity of the information.
A type of access control on the matrix.

Clearing House:
* * * a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. (HIPAA, Subtitle F, Section 262(a) Section 1171(2))

Combination locks changed:
Documented procedure for changing combinations of locking mechanisms, both on a recurring basis and when personnel knowledgeable of combinations no longer have a need to know or a requirement for access to the protected facility/system.
Part of termination procedures on the matrix.

Confidentiality:
The property that information is not made available or disclosed to unauthorized individuals, entities or processes. (ISO 7498–2, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems) .

Context-based access:
An access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The ''external'' factors might include time of day, location of the user, strength of user authentication, etc.
Part of access control on the matrix.

Contingency Plan:
A plan for responding to a system emergency. The plan includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster. (O'Reilly, 1992, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems) Contingency plans should be updated routinely.
Part of Administrative procedures to guard data integrity, confidentiality and availability on the matrix.

Continuity of signature capability:
The public verification of a signature shall not compromise the ability of the signer to apply additional secure signatures at a later date. (ASTM E 1762—95)

Part of digital signature on the matrix.

Counter signatures:
It shall be possible to prove the order of application of signatures. This is analogous to the normal business practice of countersignatures, where some party signs a document which has already been signed by another party. (ASTM E 1762 -95)
Part of digital signature on the matrix.

Data:
A sequence of symbols to which meaning may be assigned. (NRC, 1991, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)

Data authentication:
The corroboration that data has not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, double keying, a message authentication code, or digital signature.
Part of technical security services to control and monitor access to information on the matrix

Data backup:
A retrievable, exact copy of information.
Part of media controls on the matrix.

Data backup plan:
A documented and routinely updated plan to create and maintain, for a specific period of time, retrievable exact copies of information.
Part of contingency plans on the matrix.

Data Integrity:
The property that dat has [sic] not been altered or destroyed in an unauthorized manner. (ASTM E1762–95).

Data storage:
The retention of health care information pertaining to an individual in an electronic format.
Part of media controls on the matrix.

Digital signature:
An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. (FDA Electronic Record; Electronic Signatures; Final Rule)
Part of electronic signature on the matrix.

Disaster recovery:
The process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure. (CPRI, 1996c, as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)
Part of physical access controls (limited access) on the matrix.

Disaster recovery plan:
Part of an overall contingency plan. The plan for a process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure. (CPRI, 1996c, as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)
Part of contingency plan on the matrix.

Discretionary access control:
Discretionary Access Control (DAC) is used to control access by restricting a subject's access to an object. It is generally used to limit a user's access to a file. In this type of access control it is the owner of the file who controls other users' accesses to the file.
A type of access control on the matrix.

Disposal:
The final disposition of electronic data, and/or the hardware on which electronic data is stored.
Part of media controls on the matrix.

Documentation:
Written security plans, rules, procedures, and instructions concerning all components of an entity's security.
Part of security configuration mgmt on the matrix.

Electronic data interchange (EDI):
Intercompany, computer-to-computer transmission of business information in a standard format. For EDI purists, ''computer-to-computer'' means direct transmission from the originating application program to the receiving, or processing, application program, and an EDI transmission consists only of business data, not any accompanying verbiage or free-form messages. Purists might also contend that a standard format is one that is approved by a national or international standards organization, as opposed to formats developed by industry groups or companies. (EDI Security, Control, and Audit)

Electronic signature:
The attribute that is affixed to an electronic document to bind it to a particular entity. An electronic signature process secures the user authentication (proof of claimed identity, such as by biometrics (fingerprints, retinal scans, hand written signature verification, etc.), tokens or passwords) at the time the signature is generated; creates the logical manifestation of signature (including the possibility for multiple parties to sign a document and have the order of application recognized and proven) and supplies additional information such as time stamp and signature purpose specific to that user; and ensures the integrity of the signed document to enable transportability, interoperability, independent verifiability, and continuity of signature capability. Verifying a signature on a document verifies the integrity of the document and associated attributes and verifies the identity of the signer. There are several technologies available for user authentication, including passwords, cryptography, and biometrics. (ASTM 1762–95, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)

Emergency mode operation:
Access controls in place that enable an enterprise to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
Part of physical access controls (limited access) on the matrix.

Emergency mode operation plan:
Part of an overall contingency plan. The plan for a process whereby an enterprise would be able to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
Part of contingency plan on the matrix.

Encryption:
Transforming confidential plaintext into ciphertext to protect it. Also called encipherment. An encryption algorithm combines plaintext with other values called keys, or ciphers, so the data becomes unintelligible. Once encrypted, data can be stored or transmitted over unsecured lines. (EDI Security, Control, and Audit)
Decrypting data reverses the encryption algorithm process and makes the plaintext available for further processing.
Part of access control on the matrix.

Entity authentication:
1. The corroboration that an entity is the one claimed. (ISO 7498–2, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)
Part of technical security services to control and monitor access to information on the matrix.
2. A communications/network mechanism to irrefutably identify authorized users, programs, and processes, and to deny access to unauthorized users, programs and processes.
Part of mechanisms to prevent unauthorized access to data that is transmitted over a communications network on the matrix.

Equipment control (into and out of site):
Documented security procedures for bringing hardware and software into and out of a facility and for maintaining a record of that equipment. This includes, but is not limited to, the marking, handling, and disposal of hardware and storage media.
Part of physical access controls (limited access) on the matrix.

Facility security plan:
A plan to safeguard the premises and building(s) (exterior and interior) from unauthorized physical access, and to safeguard the equipment therein from unauthorized physical access, tampering, and theft.
Part of physical access controls (limited access) on the matrix.

Formal mechanism for processing records:
Documented policies and procedures for the routine, and non-routine, receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information.

Part of administrative procedures to guard data integrity, confidentiality, and availability on the matrix.

Hardware/software installation & maintenance review and testing for security features:
Formal, documented procedures for (1) connecting and loading new equipment and programs, (2) periodic review of the maintenance occurring on that equipment and programs, and (3) periodic security testing of the security attributes of that hardware/software.
Part of security configuration mgmt on the matrix.

Independent verifiability:
The capability to verify the signature without the cooperation of the signer. Technically, it is accomplished using the public key of the signatory, and it is a property of all digital signatures performed with asymmetric key encryption
Part of digital signature on the matrix.

Information:
Data to which meaning is assigned, according to context and assumed conventions. (National Security Council, 1991, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)

Information access control:
Formal, documented policies and procedures for granting different levels of access to health care information.
Part of administrative procedures to ensure integrity and confidentiality on the matrix.

Integrity controls:
Security mechanism employed to ensure the validity of the information being electronically transmitted or stored.
Part of mechanisms to prevent unauthorized access to data that is transmitted over a communications network on the matrix.

Internal audit:
The in-house review of the records of system activity (for example, logins, file accesses, security incidents) maintained by an organization.
Part of administrative procedures to guard data integrity, confidentiality, and availability on the matrix.

Interoperability:
The applications used on either side of a communication, between trading partners and/or between internal components of an entity, being able to read and correctly interpret the information communicated from one to the other.
Part of digital signature on the matrix.

Inventory:
Formal, documented identification of hardware and software assets.
Part of security configuration mgmt on the matrix.

Key:
An input that controls the transformation of data by an encryption algorithm (NRC, 1991, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)

Maintenance of record of access authorizations:
Ongoing documentation and review of the levels of access granted to a user, program, or procedure accessing health information.
Part of personnel security on the matrix.

Maintenance records:
Documentation of repairs and modifications to the physical components of a facility, for example, hardware, software, walls, doors, locks.
Part of physical access controls (limited access) on the matrix.

Mandatory Access Control (MAC):
A means of restricting access to objects that is based on fixed security attributes assigned to users and to files and other objects. The controls are mandatory in the sense that they cannot be modified by users or their programs. (Stallings, 1995) (as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)
A type of access control on the matrix.

Media controls:
Formal, documented policies and procedures that govern the receipt and removal of hardware/software (for example, diskettes, tapes) into and out of a facility.
Part of physical safeguards to guard data integrity, confidentiality, and availability on the matrix.

Message:
A digital representation of information. (ABA Digital Signatures Guidelines)

Message authentication:
Ensuring, typically with a message authentication code, that a message received (usually via a network) matches the message sent. (O'Reilly, 1992, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)
Part of mechanisms to prevent unauthorized access to data that is transmitted over a communications network on the matrix

Message authentication code:
Data associated with an authenticated message that allows a receiver to verify the integrity of the message. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)

Message integrity:
The assurance of unaltered transmission and receipt of a message from the sender to the intended recipient. (ABA Digital Signature Guidelines)
Part of digital signature on the matrix.

Multiple signatures:
It shall be possible for multiple parties to sign a document. Multiple signatures are conceptually, simply appended to the document. (ASTM E 1762–95)
Part of digital signature on the matrix.

Need-to-know procedures for personnel access:
A security principle stating that a user should have access only to the data he or she needs to perform a particular function. (O'Reilly, 1992, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)
Part of physical access controls (limited access) on the matrix.

Nonrepudiation:
Strong and substantial evidence of the identity of the signer of a *message* and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents. (ABA Digital Signature Guidelines)
Part of digital signature on the matrix.

Operating, and in some cases, maintenance personnel have proper access authorizations:
Formal, documented policies and procedures to be followed in determining the access level to be granted to individuals working on, or in the vicinity of, health information.
Part of personnel security on the matrix.

Password:
Confidential authentication information composed of a string of characters. (ISO 7498—2, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)
Part of entity authentication on the matrix.

Periodic security reminders:
Employees, agents and contractors should be made aware of security concerns on an ongoing basis.
Part of training on the matrix.

Personnel clearance procedure:
A protective measure applied to determine that an individual's access to sensitive unclassified automated information is admissible. 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 screening processes are applied in such a way as to allow a range of implementation, from minimal procedures to more stringent procedures commensurate with the sensitivity of the data to be accessed and the magnitude of harm or loss that could be caused by the individual (DOE 1360.2A, as cited in Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
Part of personnel security on the matrix.

Personnel security:
The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances. (NCSC Glossary of Computer Security Terms, October 21, 1988)
Part of administrative procedures to guard data integrity, confidentiality and availability on the matrix.

Personnel security policy/procedure:
Formal, documentation of policies and procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
Part of personnel security on the matrix.

Physical access controls (limited access):
Those formal, documented policies and procedures to be followed to limit

physical access to an entity while ensuring that properly authorized access is allowed.
Part of Physical safeguards to guard data integrity, confidentiality, and availability on the matrix.

Physical safeguards:
Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Also covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities. (O'Reilly, 1992, as cited in HISB, draft Glossary of Terms Related to Information Security in Health Care Information Systems)
A section of the matrix covering physical security requirements.

PIN (Personal Identification Number):
A number or code assigned to an individual and used to provide verification of identity.
Part of entity authentication on the matrix.

Policy/guideline on work station use:
Documented instructions/procedures delineating 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 computer terminal site or type of site, dependant upon the sensitivity of the information accessed from that site.
Part of Physical safeguards to guard data integrity, confidentiality, and availability on the matrix.

Procedure for emergency access:
Documented instructions for obtaining necessary information during a crisis.
Part of access control on the matrix.

Procedures for verifying access authorizations prior to physical access:
Formal, documented policies and instructions for validating the access privileges of an entity prior to granting those privileges.
Part of physical access controls (limited access) on the matrix.

Provider:
A supplier of services as defined in section 1861(u) of the HIPAA.
A supplier of medical or other services as defined in section 1861(s) of the HIPAA.

Public key:
One of the two keys used in an asymmetric encryption system. The public key is made public, to be used in conjunction with a corresponding private key. [Stallings, 1995]

Removal from access lists:
The physical eradication of an entity's access privileges.
Part of termination procedures on the matrix.

Removal of user account(s):
The termination or deletion of an individual's access privileges to the information, services, and resources for which they currently have clearance, authorization, and need-to-know when such clearance, authorization and need-to-know no longer exists.
Part of termination procedures on the matrix.

Report procedures:
The documented formal mechanism employed to document security incidents.
Part of security incident procedures on the matrix.

Response procedures:
The documented formal rules/instructions for actions to be taken as a result of the receipt of a security incident report.
Part of security incident procedures on the matrix.

Risk analysis:
Risk analysis, a process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.
Part of the security management process on the matrix.

Risk management:
Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. (NIST Pub. 800–14)
Part of the security management process on the matrix.

Role-based access control:
Role-based access control (RBAC) is an alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. With RBAC, rather than attempting to map an organization's security policy to a relatively low-level set of technical controls (typically, access control lists), each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.
Part of access control on the matrix.
Part of authorization control on the matrix.

Sanction policy:
Organizations must have policies and procedures regarding disciplinary actions which are communicated to all employees, agents and contractors, for example, verbal warning, notice of disciplinary action placed in personnel files, removal of system privileges, termination of employment and contract penalties (ASTM E 1869)
In addition to enterprise sanctions, employees, agents, and contractors must be advised of civil or criminal penalties for misuse or misappropriation of health information. Employees, agents and contractors, must be made aware that violations may result in notification to law enforcement officials and regulatory, accreditation and licensure organizations. (ASTM)
Part of the security management process on the matrix.

Secure work station location:
Physical safeguards to eliminate or minimize the possibility of unauthorized access to information, for example, locating a terminal used to access sensitive information in a locked room and restricting access to that room to authorized personnel, not placing a terminal used to access patient information in any area of a doctor's office where the screen contents can be viewed from the reception area.
Part of physical safeguards to guard data integrity, confidentiality, and availability on the matrix.

Security:
Security encompasses all of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster preparedness, and the oversight of all these areas. The purpose of security is to protect both the system and the information it contains from unauthorized access from without and from misuse from within.
Through various security measures, a health information system can shield confidential information from unauthorized access, disclosure and misuse, thus protecting privacy of the individuals who are the subjects of the stored data. (Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality)

Security awareness training:
All employees, agents, and contractors must participate in information security awareness training programs. Based on job responsibilities, individuals may be required to attend customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security. (ASTM)
Part of Physical safeguards to guard data integrity, confidentiality, and availability on the matrix.

Security configuration management:
Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practices and procedures of the organization so as to create a coherent system of security. (OECD Guidelines, as cited in NIST Pub 800–14)
Part of administrative procedures to guard data integrity, confidentiality, and availability on the matrix.

Security incident procedures:
Formal, documented instructions for reporting security breaches.
Part of administrative procedures to guard data integrity, confidentiality and availability on the matrix.

Security management process:
A security management process encompasses the creation, administration and oversight of policies to ensure the prevention, detection, containment, and correction of security breaches. It involves risk analysis and risk management, including the establishment of accountability, management controls (policies and education), electronic controls, physical security, and penalties for the abuse and misuse of its assets, both physical and electronic.

Part of administrative procedures to guard data integrity, confidentiality and availability on the matrix.

Security policy:
The framework within which an organization establishes needed levels of information security to achieve the desired confidentiality goals. A policy is a statement of information values, protection responsibilities, and organization commitment for a system. (OTA, 1993) The American Health Information Management Association recommends that security policies apply to all employees, medical staff members, volunteers, students, faculty, independent contractors, and agents. (AHIMA, 1996c) (as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)
Part of the security management process on the matrix

Security testing:
A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed applications environment. This process includes hands-on functional testing, penetration testing, and verification. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
Part of security configuration mgmt on the matrix.

Sign-in for visitors and escort, if appropriate:
Formal, documented procedure governing the reception and hosting of visitors.
Part of physical access controls (limited access) on the matrix.

Subject/object separation:
Access to a subject does not guarantee access to the objects associated with that subject.
Subject is defined as an active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
Object is defined as a passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
A type of access control.

System users, including maintenance personnel, trained in security:
See Awareness training (including management).
Part of personnel security on the matrix.

Technical security mechanisms:
The processes that are put in place to guard against unauthorized access to data that is transmitted over a communications network,
A section of the matrix.

Technical security services:
The processes that are put in place (1) to protect information and (2) to control and monitor individual access to information.
A section of the matrix.

Telephone callback:
A method of authenticating the identity of the receiver and sender of information through a series of ''questions'' and ''answers'' sent back and forth establishing the identity of each. For example, when the communicating systems exchange a series of identification codes as part of the initiation of a session to exchange information, or when a host computer disconnects the initial session before the authentication is complete, and the host calls the user back to establish a session at a predetermined telephone number.
Part of Entity authentication on the matrix.

Termination procedures:
Formal, documented instructions, which include appropriate security measures, for the ending of an employee's employment, or an internal/external user's access.
Part of administrative procedures to guard data integrity, confidentiality and availability on the matrix.

Testing and revision:
(1) Testing and revision of contingency plans refers to the documented process of periodic testing to discover weaknesses in such plans and the subsequent process of revising the documentation if necessary.
Part of contingency plan on the matrix.
(2) Testing and revision of programs should be restricted to formally authorized personnel.
Part of physical access controls (limited access) on the matrix.

Time-of-day:
Access to data is restricted to certain time frames, e.g., Monday through Friday, 8:00 a.m. to 6:00 p.m.
A type of access control on the matrix.

Time-stamp:
To create a notation that indicates, at least, the correct date and time of an action, and the identity of the person that created the notation.

Token:
A physical item that's used to provide identity. Typically an electronic device that can be inserted in a door or a computer system to obtain access. (O'Reilly, 1992) (as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)
Part of entity authentication on the matrix

Training:
Education concerning the vulnerabilities of the health information in an entity's possession and ways to ensure the protection of that information.
Part of administrative procedures to guard data integrity, confidentiality and availability on the matrix.

Transportability:
A signed document can be transported (over an insecure network) to another system, while maintaining the integrity of the document.
Part of digital signature on the matrix.

Turn in keys, token or cards that allow access:
Formal, documented procedure to ensure all physical items that allow a terminated employee to access a property, building, or equipment are retrieved from that employee, preferably prior to termination.
Part of termination procedures on the matrix.

Unique user identification:
The combination name/number assigned and maintained in security procedures for identifying and tracking individual user identity. (ASTM)
Part of Entity authentication on the matrix.

User authentication:
The provision of assurance of the claimed identity of an entity. (ASTM E1762–5)
Part of digital signature on the matrix.

User-based access:
A security mechanism used to grant users of a system access based upon the identity of the user.
Part of access control on the matrix.
Part of authorization control on the matrix.

User education in importance of monitoring log in success/failure, and how to report discrepancies:
Training in the user's responsibility to ensure the security of health care information.
Part of training on the matrix.

User education concerning virus protection:
Training relative to user awareness of the potential harm that can be caused by a virus, how to prevent the introduction of a virus to a computer system, and what to do if a virus is detected.
Part of training on the matrix.

User education in password management:
A type of user training in the rules to be followed in creating and changing passwords and the need to keep them confidential.
Part of training on the matrix.

Virus checking:
A computer program that identifies and disables:
(1) another ''virus'' computer program, typically hidden, that attaches itself to other programs and has the ability to replicate. (Unchecked virus programs result in undesired side effects generally unanticipated by the user.)
(2) A type of programmed threat. A code fragment (not an independent program) that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources which are then not available to authorized users. (O'Reilly, 1992, as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information

Security in Health Care Information Systems)

(3) Code embedded within a program that causes a copy of itself to be inserted in one or more other programs. In addition to propagation, the virus usually performs some unwanted function. (Stallings, 1995, as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)

Part of security configuration mgmt on the matrix.

Acronyms

ABA American Bar Association
ADA American Dental Association
ANSI American National Standards Institute
AHIMA American Health Information Management Association
ASTM American Society for Testing and Materials
CDT Center for Democracy & Technology
CEN Central European Nations
CORBA Common Object Request Broker
CPRI Computer-based Patient Record Institute
DAC Discretionary Access Control
DEA Data Encryption Algorithm
EDI Electronic Data Interchange
EHNAC Electronic Healthcare Network Accreditation Commission
FDA Food and Drug Administration
HISB Health Care Informatics Standards Board
ISO International Organization for Standardization
MAC Mandatory Access Control
NCSC National Computer Security Center
NCQA National Council for Quality Assurance
NCVHS National Committee on Vital and Health Statistics
NUBC National Uniform Billing Committee
NUCC National Uniform Claim Committee
PGP Pretty Good Privacy
PIN Personal Identification Number
NIST National Institutes of Standards and Technology
SDO Standards Development Organization
WEDI Workgroup for Electronic Data Interchange

Bibliography

ABA, Digital Signature Guidelines.
ANSI, ASC X12.58, Security Structures, June, 1997.
ASTM, E1762–95, Standard Guide for Electronic Authentication of Health Care Information. ASTM Committee E–31 on Computerized Systems, Subcommittee E31.20 on Authentication. West Conshohocken, PA, October 10, 1995.
ASTM, A Security Framework for Healthcare Information. ASTM Committee E–31 on Computerized Systems, Subcommittee E31.20 on Authentication. West Conshohocken, PA, February 11, 1997.
EDI Security, Control, and Audit, Marcells, Albert J. & Chan, Sally. Artech House, 685 Canton Street, Norwood, MA 01602, 1993.
FDA, Electronic Record; Electronic Signatures; Final Rule.
For the Record—Protecting Electronic Health Information, Computer Science and Telecommunications Board, NRC, National Academy Press, 2102 Constitution Avenue, NW, Box 285, Washington, DC, 20055, 1997.
Glossary of INFOSEC and INFOSEC Related Terms, Version 6. Schou, Corey D., Center for Decision Support, Idaho State University. August, 1996
HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS Glossary of Terms Related to Information Security in Health Care Information Systems draft, 1997
NCSC, Glossary of Computer Security Terms, October 21, 1988.
NIST Pub 800–14, ''Generally Accepted Principles and Practices for Securing Information Technology Systems'', Swanson, Marianne, & Guttman, Barbara, September, 1996. PGP, Inc., Cryptology Reference Chart, August, 1997
Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality, Goldman, Janlori & Mulligan, Deirdre, CDT, 1996.

Addendum 3

HIPAA SECURITY MATRIX—mapping

Please Note: While we have attempted to categorize security requirements for ease of understanding and reading clarity, there are overlapping areas on the matrix in which the same requirements are restated in a slightly different context.

ADMINISTRATIVE PROCEDURES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation	Mapped standards
Certification		47.
Chain of trust partner agreement		12, 47.
Contingency plan (all listed implementation features must be implemented).	Applications and data criticality analysis	17, 47, 53.
	Data backup plan	12, 17, 47.
	Disaster recovery plan	12, 17, 47, 53.
	Emergency mode operation plan	47, 53.
	Testing and revision	12, 17, 47.
Formal mechanism for processing records		12, 17.
Information access control (all listed implementation features must be implemented).	Access authorization	12, 17, 47, 53.
	Access establishment	17, 47, 53.
	Access modification	12, 17, 47, 53.
Internal audit		12, 17, 43, 44, 47.
Personnel security (all listed implementation features must be implemented)	Assure supervision of maintenance personnel by authorized, knowledgeable person.	17, 47.
	Maintainance of record of access authorizations.	12, 17, 47.
	Operating, and in some cases, maintenance personnel have proper access authorization.	17, 47.
	Personnel clearance procedure	17, 47.
	Personnel security policy/procedure	17, 47, 53.
	System users, including maintenance personnel, trained in security.	12, 17, 47, 53.
Security configuration mgmt. (all listed implementation features must be implemented).	Documentation	12, 17, 47, 53.
	Hardware/software installation & maintenance review and testing for security features.	12, 17, 47.
	Inventory	12, 17.
	Security testing	12, 17, 47.
	Virus checking	12, 17, 47, 53.
Security incident procedures (all listed implementation features must be implemented).	Report procedures	12, 17, 47.
	Response procedures	17, 47.

ADMINISTRATIVE PROCEDURES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY—Continued

Requirement	Implementation	Mapped standards
Security management process (all listed implementation features must be implemented).	Risk analysis	12, 17, 47, 53.
	Risk management	17, 47.
	Sanction policy	12, 17, 47, 53.
	Security policy	17, 47, 53.
Termination procedures (all listed implementation features must be implemented).	Combination locks changed	12, 17.
	Removal from access lists	12, 17, 47, 53.
	Removal of user account(s)	12, 17, 47.
	Turn in keys, token or cards that allow access	12, 17, 47.
Training (all listed implementation features must be implemented).	Awareness training for all personnel (including mgmt).	12, 17, 18, 47, 53.
	Periodic security reminders	12, 18.
	User education concerning virus protection	
	User education in importance of monitoring log in success/failure, and how to report discrepancies.	12, 17, 18.
	User education in password management	12, 18, 47

PHYSICAL SAFEGUARDS TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation	Mapped standards
Assigned security responsibility		47.
Media controls (all listed implementation features must be implemented).	Access control	17, 47, 53.
	Accountability (tracking mechanism)	17, 18, 47.
	Data backup	12, 17, 47, 53.
	Data storage	12, 17, 47.
	Disposal	17, 47, 53.
Physical access controls (limited access) (all listed implementation features must be implemented).	Disaster recovery	17.
	Emergency mode operation	17.
	Equipment control (into and out of site)	17, 47.
	Facility security plan	12, 17, 47.
	Procedures for verifying access authorizations prior to physical access.	17, 18, 47.
	Maintenance records	17
	Need-to-know procedures for personnel access.	12, 17, 47, 53
	Sign-in for visitors and escort, if appropriate	17
	Testing and revision	17, 47
Policy/guideline on work station use		18.
Secure work station location		17, 53.
Security awareness training		12, 17, 47.

TECHNICAL SECURITY SERVICES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation	Mapped standards
Access control (The following implementation feature must be implemented: Procedure for emergency access, In addition, at least one of the following three implementation features must be implemented: Context-based access, Roll-based access, User-based access. The use of Encryption is optional).	Context-based access,	5, 12, 14, 16, 17, 40, 47.
	Encryption	1, 6, 12, 14, 17, 21, 22, 23, 24, 26, 36, 28, 29, 30, 31, 47, 49, 53, 54, 55.
	Procedure for emergency access	14, 17, 53.
	Roll-based access,	14, 16, 17, 40, 41, 47, 53.
	User-based access.	11, 12, 14, 16, 17, 40, 41, 47, 53.
Audit controls		12, 14, 18, 47, 53.
Authorization control (At least one of the listed implementation features must be implemented).	Role-based access	5, 14, 16, 17, 47, 53.
	User-based access	14, 16, 47, 53.
Data authentication		11, 53.
Entity Authentication (The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented).	Automatic logoff	14, 16, 17, 18, 40, 53
	Biometric	14, 16, 18, 40, 47, 53.
	Password	14, 16, 17, 18, 19, 40, 47, 53.
	PIN	14, 16, 18, 19, 40, 47.
	Telephone callback	14, 17, 18, 47, 53.
	Token	14, 17, 47, 50, 53.
	Unique user identification	14, 47, 53.

TECHNICAL SECURITY MECHANISMS TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation	Mapped standards
Communications/network controls (If communications or networking is employed, the following implementation features must be implemented: Integrity controls, Message authentication. In addition, one of the following implementation features must be implemented: Access controls, Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting).	Access controls	14, 17, 22, 23, 39, 47, 48, 53.
	Alarm, event reporting, and audit trail	14, 17, 18, 35, 36, 37, 38, 44.
	Audit trail	
	Encryption	1, 6, 12, 14, 17, 21, 22, 23, 24, 26, 27, 28, 29, 30, 31, 47, 49, 52, 53.
	Entity authentication	12, 14, 17, 18, 20, 22, 23, 31, 32, 33, 34, 51, 53.
	Event reporting	
	Integrity controls	14, 15, 17, 18, 22, 23, 45, 46.
	Message authentication	14, 15, 17, 18, 22, 23, 25, 45, 46, 52.

ELECTRONIC SIGNATURE

Requirement	Implementation	Mapped standards
Digital signature (If digital signature is employed, the following three implementation features must be implemented: Message integrity, Non-repudiation, User authentication. Other implementation features are optional).	Ability to add attributes	3, 4, 10, 11, 13, 20
	Continuity of signature capability	3, 4, 11, 13, 14, 18
	Counter signatures	3, 4, 10, 11, 13, 14, 18
	Independent verifiability	3, 4, 11, 13, 20
	Interoperability	3, 4, 7, 8, 9, 13, 14, 48
	Message integrity	3, 4, 10, 11, 13, 14, 18
	Multiple signatures	3, 4, 10, 11, 13, 20
	Non-repudiation	2, 3, 4, 10, 11, 13, 14, 42
	Transportability	3, 4, 11, 13, 14, 18
	User authentication	3, 4, 10, 11, 13, 20

Mapped Standards

1. ANSI X3.92—Data Encryption Standard
2. ANSI X9.30—Part 1: Public Key Cryptography Using Irreversible Algorithms: Digital Signature Algorithm
3. ANSI X9.30—Part 2: Public Key Cryptography Using Irreversible Algorithms: Secure Hash Algorithm (SHA–1)
4. ANSI X9.31—Reversible Digital Signature Algorithms
5. ANSI X9.45—Enhanced Management Controls Using Digital Signatures and Attribute Certificates
6. ANSI X9.52—Triple DES Modes of Operation
7. ANSI X9.55—Extensions to Public Key Certificates and CRLs
8. ANSI X9.57—Certificate Management
9. ANSI X9.62—Elliptic Curve Digital Signature Algorithm (draft)
10. ANSI X12.58—Security Structures (version 2)
11. ASTM E 1762—Standard Guide for Authentication of Healthcare Information
12. ASTM E 1869—Draft Standard for Confidentiality, Privacy, Access and Data Security Principles
13. ASTM PS 100–97—Standard Specification for Authentication of Healthcare Information Using Digital Signatures
14. ASTM PS 101–97—Security Framework for Healthcare Information
15. ASTM PS 102–97—Standard Guide for Internet and Intranet Security
16. ASTM PS 103–97 Authentication & Authorization Guideline
17. CEN—European Pre-Standard
18. FDA—Electronic Records—Electronic Signatures—Final Rule
19. FIPS PUB 112—Password Usage
20. FIPS PUB 196—Entity Authentication Using Public Key Cryptography
21. FIPS PUB 46–2—Data Encryption Standard
22. IEEE 802.10: Interoperable LAN/MAN Security (SILS), 1992–1996 (multiple parts)
23. IEEE 802.10c—LAN/WAN Security—Key Management
24. IETF ID—Combined SSL/PCT Transport Layer Security Protocol
25. IETF ID—FTP Authentication Using DSA
26. IETF ID—Secure HyperText TP Protocol (S–HTTP)
27. IETF ID—SMIME Cert Handling
28. IETF ID—SMIME Message Specification
29. IETF RFC 1422—Privacy Enhanced Mail: Part 1: Message Encryption and Authentication Procedures
30. IETF RFC 1424—Privacy Enhanced Mail: Part 2: Certificate-Based Key Management
31. IETF RFC 1423—Privacy Enhanced Mail: Part 3: Algorithms, Modes, and Identifiers
32. ISO/IEC 9798–1: Information Technology—Security Techniques—Entity Authentication Mechanisms—Part 1: General Model
33. ISO/IEC 9798–2: Information Technology—Security Techniques—Entity Authentication Mechanisms—Part 2: Entity Authentication Using Asymmetric Techniques
34. ISO/IEC 9798–2: Information Technology—Security Techniques—Entity Authentication Mechanisms—Part 2: Entity Authentication Using Symmetric Techniques
35. ISO/IEC 10164–4—Information Technology—Open Systems Connection—System Management: Alarm Reporting Function
36. ISO/IEC 10164–5—Information Technology—Open Systems Connection—System Management: Event Report Management Function
37. ISO/IEC 10164–7—Information Technology—Open Systems Connection—System Management: Security Alarm Reporting Function
38. ISO/IEC 10164–8—Information Technology—Open Systems Connection—System Management: Security Audit Trail Function
39. ISO/IEC 10164–9—Information Technology—Open Systems Connection—System Management: Objects and Attributes for Access Control
40. ISO/IEC 10181–2—Information Technology—Security Frameworks in Open Systems—Authentication Framework
41. ISO/IEC 10181–3—Information Technology—Security Frameworks in Open Systems—Access Control Framework
42. ISO/IEC 10181–4—Information Technology—Security Frameworks in Open Systems—Non-repudiation Framework
43. ISO/IEC 10181–5—Information Technology—Security Frameworks in Open Systems—Confidentiality Framework
44. ISO/IEC 10181–7—Information Technology—Security Frameworks in Open Systems—Security Audit Framework
45. ISO/IEC 10736—Information Technology—Telecommunications and Information Exchange Between Systems—Transport Layer Security Protocol (TLSP)

46. ISO/IEC 11577—Information Technology—Telecommunications and Information Exchange Between Systems—Network Layer Security Protocol (NLSP)
47. NIST—Generally Accepted Principles and Practices for Secure Information Technology Systems
48. NIST MISPC—Minimum Interoperability Specification for PKI Components Version 1
49. PKCS #7—Cryptographic Message Syntax Standard Version 1.5 or later
50. PKCS #11—Cryptoki B A Cryptographic Token Interface
51. RFC 1510—Kerberos Authentication Service
52. RFC 2104—HMAC:Keyed-Hashing for Message Authentication
53. For the Record—Protecting Electronic Health Information
54. ANSI X9.42—Management of Symmetric Keys Using Diffie-Hellman
55. ANSI X9.44—Key Transport Using RSA

[FR Doc. 98–21601 Filed 8–7–98; 1:23 pm]

BILLING CODE 4120–01–P