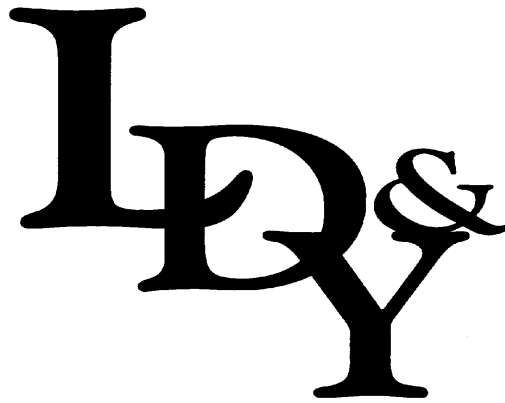


# HIPAA

## PROPOSED SECURITY STANDARD



*Prepared by*

**Kimber L. Latsha, Esq.**  
**David C. Marshall, Esq.**

The information herein reflects the views of the author. The information should be construed as general guidelines and not interpreted as legal advice. The materials should serve as a general reference to facilitate more thorough research and analysis with the assistance of a competent professional who would have an opportunity to consider the facts of any particular situation.

## I. SUMMARY

- A. The Rule proposes standards for the *security* of individual health information and electronic signature use by health plans, health care clearing houses and health care providers. The security standards would be used to develop and maintain the security of *all electronic* individual health information. Conversely, the electronic signature standard would be applicable only for the specific transactions defined in HIPAA, and only when an electronic signature must be used.
- B. The use of the security and electronic signature standards is designed to 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.
- C. The security standard to be adopted under the administrative simplification provisions of the Act is *not* restricted to the transactions referred to in the Act, but is applicable to any health information pertaining to an individual that is electronically maintained or transmitted. The legislation requires the secretary of HHS to establish security standards for health care information systems.

## II. APPLICABILITY OF THE PROPOSED RULE

- A. The security provisions of the proposed rule apply to any health plan, any health care clearing house, and any *health care provider* that electronically maintains or transmits any health information relating to an *individual*.
- B. The security regulation applies to each health care provider electronically maintaining or transmitting any health information pertaining to an individual, even if the health care provider does not transmit any of the specific standard transactions referenced in HIPAA.
- C. 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.
- D. The proposed rule does not mandate the use of electronic signatures with any specific transaction at this time.

### III. THE PROPOSED SECURITY STANDARD

- A. The security standard, as proposed, 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.
- B. 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, the proposed rule, designates a new, comprehensive standard, which defines the security requirements to be fulfilled.
- C. The proposed standard does not reference or advocate specific technology because the security technology is changing quickly. Providers are to be given 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.
- D. The standard must be “scalable”. By scalable, the standard must be able to be implemented by all of the effected entities to the smallest provider to the largest clearing house.
- E. A single approach would be neither economically feasible nor effective in safeguarding health data. For example, in the small physician practice, a contingency plan for system emergencies might be only a few pages long, and cover issues such as where back-up diskettes must be stored and the location of a back-up 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’s office.
- F. The proposed rule defines the security standard as a set of requirements with implementation features that providers must include in their operations to assure that electronic health information pertaining to an individual remains secure.
- G. The standard does not address the extent to which a particular entity should implement the specific features. Instead, each effected entity is required to 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.*

- H. Each health care entity engaged in electronic maintenance or transmission of health information must assess potential risks and vulnerabilities to the individual health data in its possession in electronic form, and develop, implement, and maintain appropriate security measures.
- I. Each entity must *maintain documentation demonstrating* the development, implementation and maintenance of appropriate security measures that include, *at a minimum*, the requirements and implementation features of the proposed rule. Additionally, entities must *maintain necessary documentation to demonstrate* that these measures have been periodically reviewed, validated, updated and kept current.

#### IV. DEFINITIONS

- A. 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.
- B. Access Control: Refers to a method of restricting access to resources, allowing only privileged entities access. The types of access control include, among others, mandatory access control, discretionary control, time-of-day and classification.
- C. Authentication: Refers to the corroboration that an entity is the one claimed.
- D. Contingency Plan: Refers to a plan for responding to a system emergency. The plan includes performing back ups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency and recovering from a disaster.
- E. Encryption (or Encypherment): Refers to transforming confidential plain text into cipher text to protect it. Once encrypted, data can be stored or transmitted over unsecured lines.
- F. Password: Refers to confidential, authentication information composed of a string of characters.
- G. 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.

- H. User-Based Access: Refers to a security mechanism used to grant users of a system access based upon the identity of the user.

V. SCOPE OF THE RULE

An entity must apply the security standard to all health information pertaining to an individual that is electronically maintained or electronically transmitted.

VI. SPECIFIC REQUIREMENTS OF THE SECURITY STANDARD

Each entity *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

These are documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of the personnel in relation to the protection of data. These procedures include the following requirements:

1. Certification. Each organization would be required to conduct a technical evaluation of its computer system or network design as part of the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a specified set of security requirements. This evaluation could be performed internally or by an external, accrediting agency.
2. 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. Multiple two-party contracts (business partners) may be involved in moving information from the originating party to the ultimate receiving party. These agreements are important so that the same level of security may be maintained at all links in the chain when information moves from one organization to another.

3. Contingency Plan. A routinely, updated plan for responding to a system emergency, that includes performing back ups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering a disaster. The plan must include all of the following implementation features:
  - a. An application and data criticality analysis, which is an entity's formal assessment of the sensitivity, vulnerabilities and security of its programs and information it receives, manipulates, stores and/or transmits.
  - b. Data Back Up Plan, which is a documented and routinely updated plan to create and maintain, for a specific period of time, retrievable exact copies of information.
  - c. Disaster Recovery Plan, which is 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.
  - d. Emergency Mode Operation Plan, which is 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.
  - e. Testing and Revision Procedures, is the documented process of periodic testing of written contingency plans to discover weaknesses in the subsequent process of revising the documentation, if necessary.
4. Formal Mechanism for Processing Records. Documented policies and procedures for the routine, and non-routine receipt, manipulation, storage dissemination, transmission or disposal of health information.
5. Information Access Control. The formal documented policies and procedures for granting different levels of access to health care information, that includes all of the following implementation features.
  - a. Access Authorization, which consists of information-use policies and procedures which establish the rules for granting access, for example, to a terminal, transaction, program, process or some other user.
  - b. Access Establishment, which is security policies and rules that determine an entity's initial right of access to a terminal, transaction, program, process or some other user.
  - c. Access Modification, which is 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. The 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 must have the required authorization as well as the appropriate clearances, which includes all of the following implementation features.
  - a. 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.
  - b. Maintaining a Record of Access Authorizations (on going documentation and review of the levels of access granted to a user, program or procedure accessing health information).
  - c. 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).
  - d. Establishing personnel clearance procedures (a protective measure applied to determine that an individual's access to sensitive, unclassified, automated information is admissible).
  - e. Establishing and maintaining personnel security policies and procedures (formal, documentation of procedures to insure that all personnel who have access to sensitive information have the required authorization as well as the appropriate clearances).
  - f. 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:
  - a. Documentation consisting of written security plans, rules, procedures and instructions concerning all components of an entity's security.

- b. Hardware and software installation and maintenance review and testing for security features which consist of formal, documented procedures for connecting and loading new equipment and programs, periodic review of the maintenance occurring on the equipment and programs, and periodic security testing of the security attributes of that hardware/software.
  - c. Inventory. The formal, documented identification of hardware and software assets.
  - d. Security testing is the 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 hand-on functional testing, penetration testing and verification.
  - e. Virus checking is the act of running a computer program that identifies and disables
    - i. another virus computer program, typically hidden, that attaches itself to other programs and has the ability to replicate;
    - ii. a code fragment (not an independent program) that reproduces by attaching to another program; and
    - iii. a code embedded within a program that causes a copy of itself to be inserted in one or more programs.
9. Security Incident Procedures. Formal documented instructions for reporting security breaches, that include all of the following implementation features:
- a. Report procedures consisting of documented, formal mechanisms employed to document security incidents.
  - b. Response procedures consisting of documented, formal rules or instructions for actions to be taken as the result of the receipt of a security incident report.
10. Security Management Process. The creation, administration, and oversight of policies to insure 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:

- a. Risk Analysis. A process whereby cost-effective security/control measures may be selected by balancing the cost of various security/control measures against the losses that would be expected if these measures were not in place.
  - b. Risk Management. The process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk.
  - c. 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 the personnel files, removal of system privileges, termination of employment and contract penalties. They must include employee, agent, and contractor notice of civil and 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.
  - c. Security Policy. Statements 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 users access, that include procedures for all of the following implementation features:
- a. Changing Locks. A documented procedure for changing combinations of locking mechanisms, both on a reoccurring basis and when personnel knowledgeable of combinations no longer have a need to know or require access to the protected facility or system.
  - b. Removal from Access List. The physical eradication of an entity's access privileges.
  - c. Removal of User Accounts. 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.
  - d. Turning in of Keys, Tokens or Cards that Allow Access. The formal, documented procedure to insure 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 insure the protection of that information, that includes all of the following implementation features:
  - a. Awareness Training. 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.
  - b. Periodic Security Reminders. Employees, agents, and contractors must be made aware of security measures on an ongoing basis.
  - c. 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.
  - d. 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.
  - e. User Education and Password Management. User training in the rules to be followed in creating and changing passwords and the need to keep them confidential.

## VII. 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 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:

- A. Assigned Security Responsibility. The 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.
- B. Media Controls. The 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:

1. Access Control
  2. Accountability. The property that insures that the actions of an entity can be traced uniquely to that entity.
  3. Data Back-Up. The retrievable, exact copy of information.
  4. Data Storage. The retention of health care information pertaining to an individual in an electronic format.
  5. Disposal. The final disposition of electronic data, and/or the hardware on which electronic data is stored.
- C. Physical Access Controls. The 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:
1. Disaster Recovery. The process enabling an entity to restore any loss of data in the event of fire, vandalism, natural disaster or system failure.
  2. An Emergency Mode Operation. The access controls in place that enable an entity to continue to operate in the event of fire, vandalism, natural disaster or system failure.
  3. Equipment Control. The 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.
  4. 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.
  5. Procedures for Verifying Access Authorizations Before Granting Physical Access. The formal, document policies and instructions for validating access privileges of an entity before granting those privileges.
  6. Maintenance Records. The documentation of repairs and modifications to the physical components of a facility, such as hardware, software, walls, doors and locks.

7. 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.
  8. Procedures to Sign In Visitors and Provide Escorts. Formal, documented procedure governing the reception and hosting of visitors.
  9. Testing and Revision. The restriction of program testing and revision to formally authorized personnel.
- D. Policy and Guidelines on Workstation Use. The 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.
- E. A Secure Workstation Location. The 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 contents can be viewed from the reception area.
- F. Security Awareness Training. Information security awareness training programs in which all employees, agents, and contractors must participate, including, depending on specific job responsibilities, customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security.

## **VIII. 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:

- A. Technical Security Services, which must include *all* of the following requirements and implementation features:

1. Access Control that includes:
  - a. Procedure for Emergency Access consisting of documented instructions for obtaining necessary information during a crisis; and
  - b. at least one of the following implementation features:
    - i. 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),
    - ii. Role-Based Access
    - iii. Use-Based Access
  - c. The Optional Use of Encryption
2. Audit Controls. Mechanisms employed to record and examine system activities.
3. Authorization Controls. The mechanisms for obtaining consent for the use and disclosure of health information which includes at least one of the following implementation features:
  - a. Role-Based Access, or
  - b. User-Based Access
4. 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.
5. Entity Authentication. The corroboration that an entity is the one claimed that includes:
  - a. Automatic Log-off. A security procedure that causes an electronic session to terminate after a predetermined time of inactivity, such as 15 minutes.
  - 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:
    - i. Bio-metric identification, which is 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).

- ii. Password
- iii. Personal identification number (PIN), which consists of a number code assigned to an individual and used to provide verification of identity
- iv. Telephone call-back procedure which is 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
- v. Token

## IX. 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. If an entity uses communications or network controls, its security standards for technical security mechanisms must include the following implementation features:

- 1. Integrity Controls which consists of a security mechanism employed to insure the validity of the information being electronically transmitted or stored.
- 2. Message Authentication which is ensuring, typically with a message authentication code, that a message received (usually via network) matches the message sent.
- 3. One of the Following Implementation Features
  - a. Access Controls. The protection of sensitive communication transmissions over open or private networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient.
  - b. Encryption

B. 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:

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 an abnormality. The signal may be in any desired form ranging from a simple contact closure (or opening) to a time-phased shut down and restart cycle.
2. Audit Trail. The data collected and potentially used to facilitate a security audit.
3. 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.
4. 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.

## X. EFFECTIVE DATES

Security standard would be effective 24 months after the effective date of the final rule for the security standard (36 months for small health plans). The effective date of the final rule will be 60 days after the final rule is published in the *Federal Register*.

## XI. COST OF CONVERSION

HHS expects that most providers have already implemented some security measures and will primarily need to assess existing security, identify areas of risk and implement additional measures. HHS could not estimate the per entity cost of implementation because there was no information available regarding the extent to which providers current security practices may be deficient. *CMS believes 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.*

- A.. Implementation Options. 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. *“The security requirements are both scaleable and technically flexible.”*

- B. Quotable Quote. *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."*