



# Security Standards

## Health Insurance Portability and Accountability Act (HIPAA)

*In order to ensure privacy in a digital world, it is necessary to implement and maintain a secure environment, with secure communications and systems access, together with a classification system for data and personnel.*

Although not new to healthcare organizations, issues of security and privacy pose enormous challenges to the industry — especially in this digital age when the need to safeguard information is challenged by the need for openness, portability, and availability. Regardless, the protection of information under any organization's control is a basic responsibility, if not an out and out necessity, and the protection of an individual's privacy is mandatory. Dealt with separately and in isolation these two issues are relatively easy to address, but when included as part of the greater HIPAA standard, they are complex and require a great deal of effort and financial commitment.

The proposed HIPAA security standard states that:

*Each healthcare 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.*

The security standard defines a healthcare entity as any health plan, healthcare clearinghouse, or healthcare provider that electronically maintains or transmits any health information relating to an individual. This standard affects any organization that has "Health Information" stored electronically — regardless of whether the data is on a standalone PC, internal to a local area network, or sent across the world.

### **Information Security and Privacy**

Information security and privacy are inextricably intertwined. "Information security" refers to the physical protection of information assets, which includes everything from identifying the asset to be secured to developing relevant policies and procedures, designing the secure environment, implementing the solutions, training the staff, and testing and monitoring the system. Physical protection also serves to guarantee the integrity and availability of the data.

"Privacy" refers to the goal that secured information can be accessed and seen by authorized and certified personnel only. It is intended to preserve a patient's right to consent to the disclosure of information.

### **Security Categories**

To guarantee privacy, an organization will need to address the basic security issues. HIPAA has mapped out these security issues into a set of requirements that fall into four categories:

1. Administrative Procedures To Guard Data Integrity, Confidentiality, and Availability
2. Physical Safeguards to Guard Data Integrity, Confidentiality, and Availability
3. Technical Security Services to Guard Data Integrity, Confidentiality, and Availability
4. Technical Security Mechanisms to Guard Data Integrity, Confidentiality, and Availability

These categories were based on recommendations contained in the National Research Council's 1997 report, "For the Record: Protecting Electronic Health Information." These HIPAA requirements were developed to help organizations understand the broad scope of different elements needed to create a comprehensive, secure environment.

*continued on page 2*

## HIPAA Requirements

The state has yet to develop a standard that integrates all security issues – neither has it defined the extent to which parties must adhere to the standards, nor even defined a method for certification. This is primarily due to the fact that recognized international standards bodies, such as the American National Standards Institute (ANSI), do not have a single set of standards that address security administrative procedures, physical safeguards, technical security services, and technical mechanisms from which the standards body could work.

HIPAA presents a set of guidelines or requirements that should be implemented in order to comply with the standards. To this end the HIPAA security requirements are mapped to various international standards, with most entries having multiple standards to choose from. For example, access control is defined under “Technical Security Services to Guard Data Integrity, Confidentiality and Availability,” and has five implementation features; encryption is one of the implementation features and is subject to no less than 20 different standards.

The proposed standards provide a wide-ranging set of requirements that are technology independent, with the specific aim of allowing the standards to be flexible in order to take advantage of changing technology and practices.

A closer look at the four categories will impart a better understanding of the magnitude of work that will be needed in order to comply with HIPAA's security mandates.

### 1. Administrative Procedures to Guard Data Integrity, Confidentiality, and Availability

This category contains the required policies and formal practices that must be developed and followed in order to protect the organization's information assets. This category also defines the practices that need to be followed regarding personnel usage and conduct.

The requirements and their implementation steps, if any, follow:

Certification

Chain of trust partner agreement

Contingency plan

- 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

- Access authorization
- Access establishment
- Access modification

Internal audit

Personnel security

- Ensure supervision of maintenance personnel by authorized, knowledgeable person
- Maintenance of access authorizations record
- Operating, and in some cases, maintenance personnel have proper access authorization
- System users, including maintenance personnel, trained in security

Security configuration management

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

Security incident procedures

- Report procedures
- Response procedures

Security management process

- Risk analysis
- Risk management
- Sanction policy
- Security policy

Termination procedures

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

Training

- Awareness training for all personnel, including management
- Periodic security reminders
- User education concerning virus protection
- User education in importance of monitoring log-in success/failure and reporting discrepancies
- User education in password management

## 2. Physical Safeguards to Guard Data Integrity, Confidentiality, and Availability

This category concerns the protection of physical computer systems, and the related buildings and equipment, from natural disasters and intrusion. Physical safeguards also cover the use of administrative measures and physical measures used to control access to computer systems and facilities. The requirements follow:

Assigned security responsibility

Media controls

- Access control
- Accountability
- Data backup
- Disposal

Physical access controls

- Disaster recovery
- Emergency mode operation
- Equipment control (into and out of site)
- Facility security plan
- Procedures for verifying 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 workstation use

Secure workstation location

Security awareness training

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

This category details the processes that must be put in place to protect, control, and monitor information access. The requirements follow:

Access control (Procedure for emergency access must be implemented. In addition, at least one of the following features must be implemented, except encryption, which is optional. )

- Context-based access
- Encryption
- Procedure for emergency access
- Role-based access
- User-based access

Audit controls

Authorization control (At least one must be implemented.)

- Role-based access
- User-based access

Data authentication

Entity Authentication (Automatic logoff and unique user identification must be implemented. In addition, at least one of the remaining features must be implemented.)

- Automatic logoff
- Biometric
- Password
- PIN
- Telephone callback
- Token
- Unique user identification

## 4. Technical Security Mechanisms to Guard Data Integrity, Confidentiality, and Availability

This category relates to the processes that are to be implemented in order to prevent unauthorized access to data that is transmitted over a communications network. The requirements follow:

Communications/network controls

(If communications or networking is employed, the following features must be implemented: integrity controls and message authentication. In addition, one of either access controls or encryption must be implemented. If using a network, the following four features must be implemented: alarm, audit trail, entity authentication, and event reporting.)

- Access controls
- Alarm
- Audit trail

*continued on page 4*

- Encryption
- Entity authentication
- Event reporting
- Integrity controls
- Message authentication

### **Compliance**

The HIPAA requirements are complex and overlapping. It will require substantial efforts to plan and execute the requirements. Many healthcare organizations will not have the available, appropriate skills to tackle such a complex project, and they will be well advised to engage the services of a qualified consulting company that brings both healthcare and security expertise to ensure compliance to these requirements.

### **HIPAA and Superior**

Superior will be a leader in the digital transformation of healthcare. Our e-health services begin with strategic e-health business planning, working closely with executives to connect their current off-line business planning with on-line opportunities to electronically interact with physicians, consumers and business partners. Transforming your business also requires transforming business processes around e-commerce. This is essential to reaping the return on investment available through e-health strategies.

The technical infrastructure to implement e-health solutions includes the following aspects: network and server capabilities, security, integration in leveraging current information systems, and actual Web development. Superior has focused extensively in the area of healthcare information technology and possesses the breadth and depth of resources to leverage current investments and recommend the appropriate solutions that will support HIPAA standards.

### **Together We Can Achieve the e-Health Community**

The future of healthcare requires data standardization, security and confidentiality, and a digital transformation of our industry. Innovative CEOs who take advantage of implementing e-health strategies early will gain a competitive market position as well as show a reduction in overall costs. Superior's goal is to assist executives in leveraging current investments, understanding HIPAA legislation, and becoming a leader in the digital transformation of their organizations to better reach their consumers, physicians, and business partners.

---

For additional information, please contact:  
**Superior Consultant Holdings Corporation**  
4000 Town Center, Suite 1100  
Southfield, Michigan 48075  
(248) 386-8300  
superior@superiorconsultant.com