

Securing HIPAA Compliance: Summary of the Requirements of the Health Insurance Portability and Accountability Act's Security Regulation

Thomas H. Faris, Esq.
Chief Privacy Officer
IMPAC Medical Systems, Inc.

HIPAA is based on the concept of "Administrative Simplification," or the pursuit of the most effective and efficient use of modern information technology. Handheld computers, the Internet, e-mail communication, and the use of personal computers enable users to store nearly limitless amounts of data, perform timely searches and reporting, and distribute large quantities of information to a wide audience in practically no time.

The healthcare industry is now able to make patient records and image data instantaneously available at multiple locations, as well as provide summary analysis of multiple patient, facility, or regional studies with very little effort. HIPAA seeks to facilitate the greatest potential use of this modern technology, while providing common sense protections for the personal patient information reflected in the data.

The Security and Electronic Signature Standard ("Security") and the Privacy of Individually Identifiable Health Information Standard ("Privacy") together are intended to protect patient health information. Privacy defines the permissible means of access, use, and disclosure of the applicable patient information, while Security governs the operational and technical mechanisms necessary to protect the information.

What is information security?

Information security is a comprehensive system of actions taken to protect the confidentiality, integrity, and availability of an organization's electronic data, work product, information systems, and other related intellectual and physical property. The affirmative actions must reflect technical security devices, physical boundaries, operational policies and procedures, contingency plans, and designated personnel responsibility. These areas are defined as:

- Confidentiality – Protection of entrusted information from unauthorized use, access, or disclosure.
- Integrity – Preservation of the specific nature, character, and content of the information.
- Availability – Ability to access, use, or disclose the information as intended in an effective and efficient time, place, and manner.

Scope and Applicability of the Security Rule

Healthcare providers, health plans, and clearinghouses are charged with the legal responsibility to comply with HIPAA. The Security Rule further requires that these “covered entities” enter into chain-of-trust partner agreements with third parties that will access, use, or disclose confidential information to ensure that consistent levels of security protections are maintained. The Security rule applies to all individually identifiable health information that is either electronically stored or transmitted.

Implementation Specifics

The Security Rule requires each covered entity to assess its own operations, resources, and vulnerabilities to determine what types of security measures are necessary to protect the individually identifiable health information under its control. They must conduct careful analysis of the flow of this health information throughout their organization, and they must assess the potential risk of unauthorized access, use, or distribution of the information at all points of storage and transmission. A security gap analysis must be performed to identify the controls necessary to prevent what the entity would consider to be an unacceptable risk or vulnerability.

The rule is intended to be scalable to permit organizations to custom fit the security requirements to their particular needs. Further, the regulation is written to be technology-neutral. Covered entities must determine exactly what types and levels of security technology are appropriate to meet their security needs. This also provides for the likelihood of future technology improvements and rising industry standards.

Identifying vulnerabilities

Covered entities must assess all operations within their organization to identify all unreasonable security vulnerabilities, whether from inside or outside, intentional or unintentional, or hostile or indifferent. The Security Rule does not require the absolute prevention of all potential avenues of unauthorized use, access, or disclosure of protected information -- only those that the covered entity determines to be unreasonable. Some that must be considered are:

- Hackers trying to break into the organization’s information system;
- Interception of clear text electronic files, such as email or file transfer protocol (FTP);
- Careless password management practices;
- Curious employees reviewing specific patient records;
- Employees intentionally disclosing information to external parties;
- Malicious employees who were recently terminated or are otherwise upset with the organization;
- Security attacks via IP (Internet) ports or unprotected modems;
- Careless use of wireless devices and ports;

- Unprotected diskettes, logged in terminals, and readable data files;
- Damaged equipment, media, or electronic files; and
- Physical break-ins.

Overview of specific requirements

The Security Rule provides a specific list of minimal requirements that a covered entity must fulfill to adequately prevent unauthorized access, use, or disclosure of individually identifiable health information.

Administrative procedures

Formal operational procedures and policies must be established to provide security guidance and instruction to all applicable personnel and to ensure that all pertinent functions are consistently performed in accordance with the organization's security needs. The operational procedures shall identify organizational and specific employee job requirements surrounding the use and control of individually identifiable health information. Procedures to put in place include:

- Certification – Internal or external review and documented assurance that the organization is in compliance with the Security rule.
- Contingency Planning – Identification of potential threats to the organization and plans for continuing operations if any event occurs.
- Information Handling – Procedures for the control of protected information during pertinent operations, including designation of personnel and specific information for use.
- Access Controls – Control of the provision of authorization of information access rights.
- Internal Auditing – Internal review of operations to ensure that all security requirements are fulfilled.
- Personnel Security Authorization Control – Steps to verify authorization before granting access to protected information.
- Security Configuration Management – Comprehensive specification of the covered entity's security system.
- Incident Handling – Plans for reporting, investigating, and resolving breaches in security.
- Security Management – Analysis and mitigation of the covered entity's security vulnerabilities. Policies and plans for maintaining security, including disciplinary action.
- Employee Termination – Removal of data accessibility by terminated employees.
- Training – All personnel must be made aware of all security policies and procedures related to their job responsibilities.

Physical safeguards

The organization's buildings, equipment, and media must be protected with reasonable physical safeguards to prevent unreasonable threats to security. The covered entity must consider physical threats, such as disaster, physical or electronic break-in, burglary and theft, and careless physical access to individually identifiable health information. The covered entity must install adequate physical security protections, as well as establish operational procedures to ensure effective implementation of these protections. They include:

- Assigned Security Responsibility – Appointed responsibility for security system management.
- Media Controls – Secure handling of all media, including back-ups, storage, and transportation.
- Physical Access Controls – Maintain facilities that prevent access to terminals or networks that may permit unauthorized data access.
- Workstation Use Requirements / Accessibility Controls – Guidelines for preventing unintended data access from user workstations.

Technical security services

Operational procedures and policies must be established to restrict access to individually identifiable health information to personnel with a justifiable need to access, use, or distribute the data. These should include:

- Access Control – Access to protected information must be limited to personnel with a legitimate need for access.
- Audit Controls – Systemic tracking of access, use, and disclosure activities.
- Authorization Control – Identification of the requirement for an employee to access protected information and provision of requisite access authorization.
- Data Authentication – Verification of the integrity of the protected information.
- Entity Authentication – Verification of user identification, such as passwords or biometrics, as well as automatic logoff of vacated workstations.

Technical security mechanisms

Security technology must be implemented to protect information stored on a computer network or otherwise electronically communicated from unauthorized access, use, or distribution. Required mechanisms include:

- Integrity/Message Authentication – Assurance that the information received is identical to the information transmitted.
- Access Control – Prevention of unauthorized access to electronic communications, by either utilizing dedicated lines or encryption and a firewall.
- Alarm / Event Reporting – Intrusion detection and automatic reporting of suspicious access attempts.

- Audit Trail – Collection of data access and changes to provide for future review of the exercise of authorized access.

Technology can pose great savings in reducing the cost of healthcare operations. However, reasonable steps must be taken to preserve patient trust, satisfy regulatory requirements, and maintain the most effective and efficient health care organization.

What It Means for You

Covered entities must take immediate steps to review the flow of protected information throughout their facility and ensure that confidential information is adequately protected.

- Conduct a security gap analysis to identify your organization's vulnerabilities.
- Establish written policies and procedures that offer instruction and guidance to all employees who have access to protected health information.
- Set up safeguards to your physical plant, such as the building, equipment, and areas where protected information is kept.
- Carefully control the assignment and exercise of personnel access rights to protected information.
- Ensure that your security technology protects the storage and transmission of protected information from unreasonable risk of unauthorized interception or alteration.

Thomas H. Faris, esquire, is chief privacy officer for IMPAC Medical Systems, Inc. The company specializes in the development of practice management, electronic medical record, image management, and decision support software.