



Overview of the HIPAA Security Rule and Risk Analysis

The *Health Insurance Reform: Security Standards; Final Rule* (Security Rule) was published in the February 20, 2003 Federal Register with an effective date of April 20, 2003. Covered healthcare providers will have two full years -- until April 20, 2005 -- to comply with the standards.

The Security Rule serves as an add-on to the *Standards for Privacy of Individually Identifiable Health Information; Final Rule* (Privacy Rule), which had an implementation date of April 14, 2003. While the Privacy Rule provides standards for maintaining the confidentiality of protected health information or PHI, the Security Rule provides standards to protect the confidentiality, integrity, and availability of electronic protected health information or e-PHI.

Definitions

Protected Health Information (PHI) is defined as individually identifiable health information that is:

1. Transmitted by electronic media;
2. Maintained in electronic media; or
3. Transmitted or maintained in any other form or medium including oral.

Electronic media means:

1. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, via facsimile, and voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Electronic Protected Health Information (e-PHI) is Protected Health Information that is:

1. Transmitted by electronic media; or
2. Maintained in electronic media.

General Rule Provisions

Healthcare providers that are covered by the Rule are required to ensure the confidentiality, integrity, and availability of all e-PHI that the provider creates, receives, maintains, or transmits. In addition, a provider is required to protect against any reasonably anticipated threats or hazards to the security or integrity of e-PHI and to protect against any reasonably anticipated uses or disclosures of e-PHI that are not permitted or required under the Privacy Rule.

The Security Rule prescribes standards and implementation specifications to safeguard the confidentiality, integrity, and availability of e-PHI. The Security Rule categorizes the standards and implementation specifications into several sections: Administrative Safeguards, Physical Safeguards, Technical Safeguards, Organizational Requirements, Policies and Procedures and Documentation Requirements.

Security Standards

Administrative Safeguards - focuses on the security management process – the policies and procedures designed to prevent, detect, contain, and correct security violations. Standards include assigning security responsibility, creating policies and procedures for workforce security and information access management, security awareness and training, security incident procedures, contingency planning, and evaluation of security measures.

Physical Safeguards – focuses on protecting e-PHI from unauthorized disclosure, modification, or destruction. Standards include creating policies and procedures for facility access controls, workstation use, workstation security, and device and media controls.

Technical Safeguards – focuses on implementation of technological measures to safeguard confidentiality, integrity, and availability of e-PHI. Standards include implementation of access control measures, audit controls, integrity controls, person or entity authentication controls and transmission security measures.

Organizational Requirements – focuses on requirements for business associate contracts and group health plans.

Policies and Procedures and Documentation Requirements – focuses on the creation, documentation, review and maintenance of policies and procedures to comply with the standards, implementation specifications, or other requirements under the Security Rule.

The Security Rule is designed to be flexible and scalable to allow providers to employ various approaches and technologies to comply with the requirements.

Therefore, a provider may use any security measures that allow it to reasonably and appropriately implement the standards and implementation specifications as specified in the Rule. However, in determining which security measures to use, a provider must take into account the following factors:

1. Its size, complexity, and capabilities;
2. Its technical infrastructure, hardware, and software security capabilities;
3. The costs of security measures; and
4. The probability and criticality of potential risks to e-PHI.

Providers are required to comply with all the standards in the Rule; however, the implementation specifications are either required or addressable. If an implementation specification is addressable, a provider must:

1. Assess whether the implementation specification is a reasonable and appropriate safeguard in its environment; and
2. Either
 - a. Implement the specification if reasonable and appropriate; or
 - b. If implementing the specification is not reasonable and appropriate—
 - i. Document why it would not be reasonable and appropriate to implement the specification; and
 - ii. Implement an equivalent alternative measure if reasonable and appropriate.

Two important implementation specifications under the Administrative section are the risk analysis and risk management specifications which are required elements. These implementation specifications are integral to adequately addressing the requirements and intent of the Security Rule.

Getting Started

To begin your compliance activities, start with your internal risk analysis. The Long Term Care Consortium has created the HIPAA Risk Assessment Matrix to help you get started. For more information, refer to the following resources:

1. Risk Assessment Matrix Definitions
2. Risk Assessment Matrix
3. Policy and Procedure Overview
4. Security Standards: Matrix
5. Conducting Your Security Risk Assessment
6. Risk Assessment Matrix Instructions
7. Risk Assessment Training Program