Axian
Software Consulting and Training

How Should the Basic Security Requirements Be Met?

The security requirements must be met by applying the standards found in the Final Security Rule. The security rule standards are grouped under three headings: ***administrative safeguards***, ***physical safeguards***, and ***technical safeguards***. Compliance with the standards will be determined based on the effectiveness and feasibility of the measures in ensuring the confidentiality, integrity and availability of electronic protected health information (PHI).

Administrative Safeguards

The administrative safeguards are actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic PHI and to manage the conduct of the covered entity's workforce in relation to the protection of the information. Specifically, the administrative safeguards must address the following areas.

1. **Security Management Process:** Implement policies and procedures to prevent, detect, contain and correct security violations. There are four enumerated implementation specifications, all of which are required. These include: (a) a risk analysis to detect the potential risks and vulnerabilities; (b) risk management to implement security measures to reduce risks and vulnerabilities; (c) a sanction policy to apply appropriate sanctions against workforce members who fail to comply with the policies; and (d) information system activity review to review records of information system activity, such as audit logs, access reports and security incident tracking reports.
2. **Assigning Security Responsibility:** Identify a security official to develop and implement policies and procedures.
3. **Workforce Security:** Develop policies and procedures to ensure appropriate workforce access to electronic PHI and to prevent unauthorized access by those who should not have access to the information.
4. **Information Access Management:** Implement policies and procedures for authorizing access to electronic PHI. This includes isolating health care clearinghouse functions if they are part of a larger organization.
5. **Security Awareness and Training:** Implement a security awareness and training program for all members of the workforce (including management). The amount of training is to be determined by the covered entity.
6. **Security Incident Procedures:** Implement policies and procedures to address security incidents. This includes identifying and responding to suspected and known security incidents.
7. **Contingency Plan:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems containing electronic PHI. This requires developing and implementing a backup data plan, a disaster recovery plan and an emergency mode operation plan.

8. **Evaluation:** Perform a periodic technical and non-technical evaluation. Based initially on the standards, to assess the extent to which the entity's security policies and procedures meet the requirements of this section. The covered entity may make a business decision to obtain external certification, but is not required to do so to comply with the standard.

Physical Safeguards

Each covered entity is required to address the following physical safeguards standards that concern the physical protection of data systems and data from intrusion and from environmental or natural hazards. The physical safeguard standards are as follows:

1. **Facility Access Controls:** Implement policies and procedures to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. These controls would include the following implementation features: disaster recovery, emergency mode operation, need-to-know procedures for personnel access and sign-in requirements for visitors.

2. **Workstation Use:** Implement policies and procedures that specify 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 workstation or class of workstation that can access electronic PHI (e.g., logging off before leaving a workstation unattended).

3. **Workstation Security:** Implement physical safeguards for all work stations that access electronic PHI, to restrict access to authorized users. A risk assessment will need to be performed to gauge the appropriate solutions to workstation security issues.

4. **Device and Media Controls:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility and the movement of these items within the facility.

Technical Safeguards

The technical safeguard standards address the technology and the policies and procedures for its use that protect electronic PHI and control access to it. The following are included in the technical safeguards:

1. **Access Control:** Implement technical policies and procedures for electronic information systems (computers) that maintain electronic PHI to allow access only to those persons or software programs that have been granted access as specified by the security safeguards. This standard requires the assignment of a unique name and/or number for identifying and tracking user identity, and establishing procedures for obtaining necessary electronic PHI during an emergency. Some facilities may wish to use encryption as a method of denying access to information in a file.

2. **Audit Controls:** Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI. These are to be put in place to record and examine system activity. Entities have flexibility in implementing the standard in a manner appropriate to their needs.

3. **Integrity:** Implement policies and procedures to protect electronic PHI from improper alteration or destruction. Error-correcting memory and magnetic disc storage are

examples of the built-in data authentication mechanism that are commonplace in hardware and operating systems today.

4. **Person or Entity Authentication:** Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed. For example, digital signatures may be used to implement this standard.

5. **Transmission Security:** Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network. Integrity controls and encryption are recommended (but not required) to achieve this standard.

Documentation and Policy and Procedure Requirements

The Final Security Rule requires covered entities to implement and maintain written policies and procedures to comply with the rule. The same is true for any actions, activities or assessments required to be documented, such as the risk assessment analysis. Covered entities must maintain this documentation for six years from the later of the date of its creation or the date when it last was in effect.

Sanctions for Noncompliance

Under the HIPAA statute, violations of the Final Security Rule can result in penalties of up to $100 per person per violation, up to a maximum of $25, 000 for violations of a single standard during a calendar year. HIPAA statutory provisions also provide for criminal penalties for the knowing misuse of health identifiers or obtaining or misusing PHI of: (a) up to $50,000 and one year in prison for knowing violations; (b) up to $100,000 and up to five years in prison if the offense is committed under false pretenses; and (c) up to $250,000 and 10 years in prison if the offense is committed with “intent to sell, transfer, or use individually identifiable health information for commercial advantage, gain, or malicious harm.”

No Safe Harbors

The Final Security Rule does not offer any safe harbor provisions. Therefore, it appears that the security measures adopted and utilized by covered entities will be judged after the fact, which will make the documentation and risk analysis process all the more important.