

Overview of Requirements for the HIPAA Security Rule

The HIPAA Security Rule found in 45 CFR Parts 160, 162 and 164 provides four global requirements for covered entities:

1. Ensure the confidentiality, integrity and availability of all electronic protected health information (ePHI) that the covered entity creates, receives, maintains or transmits
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the HIPAA Privacy Rule
4. Ensure compliance by the covered entity's workforce

Specifically, we must demonstrate compliance by enacting administrative, physical and technical safeguards.

ADMINISTRATIVE SAFEGUARDS

- Create a security management process that includes risk analysis and risk management
- Conduct regular system activity reviews: audit logs, access reports, incident tracking
- Enforce workforce security through clearance procedures, authorization and access controls
- Train all workforce members on computer security awareness
- Track, report and respond to suspected or known security incidents
- Establish a contingency plan to ensure availability of ePHI during emergencies or natural disasters

PHYSICAL SAFEGUARDS

- Develop a facility security plan that limits physical access to electronic information systems to appropriate individuals and prevents tampering or theft
- Allow facility access to support disaster recovery efforts and emergency operations
- Document repairs to the physical components of the security system
- Establish allowable functions to be performed on ePHI and the physical attributes of workstations that can access ePHI
- Restrict workstation access to authorized users

- Manage the receipt, removal and disposal of hardware and electronic media

TECHNICAL SAFEGUARDS

- Use technical measures to control access to systems that maintain ePHI
- Provide for unique user identification and emergency access
- Implement audit controls that record and examine system activity
- Protect ePHI from improper alteration or destruction
- Ensure transmission security

OTHER REQUIREMENTS

- Negotiate business associate contracts with entities who provide services involving ePHI
- Document policies and procedures that support the administrative, physical and technical safeguards
- Periodically re-evaluate the organization's compliance with security requirements