

HIPAA Security Rule

Learning Objectives

- Overview of the HIPAA Security Rule via highlights of National Institute of Standards and Technology (NIST) Report
“An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule”

Learning Objectives

- Describe how the Certification Commission for Health Information Technology (CCHIT) security provisions for electronic medical records (EMRs) assure HIPAA compliance

Learning Objectives

- Look at Sample Manual Sections
- Look at Sample Training Documentation
- Look at Sample Templates

HIPAA

- The Administrative Simplification provisions of the (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for the security of electronic health care information. (1996)
- National Institute of Standards and Technology - (NIST) is responsible for developing standards and guidelines, including minimum requirements, used by federal agencies in providing adequate information security for the protection of agency operations and assets.

HIPAA Security Rule

- 2003 - HIPAA Security Rule adopted by the Secretary of Health and Human Services based on many NIST guidelines
- 2005 - Information Technology Laboratory at NIST published “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule”

HIPAA Security Rule

- Ensure the confidentiality, integrity, and availability of EPHI that an entity creates, receives, maintains, or transmits
- Protect against any reasonably anticipated threats and hazards to the security or integrity of EPHI
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

Technology

- The security standards DO NOT dictate or specify use of specific technologies
- Allows for flexibility in incorporating developing technologies

Compliance Considerations

- Size, complexity and capability of the covered entity
- The covered entities technical infrastructure, hardware and software capabilities
- The costs of security measures
- The probability and criticality of potential risks to EPHI

NIST Report Highlights

- Administrative
- Physical
- Technical
- Policy and Procedures and Documentation

Administrative

- Identify - all software and hardware
- Inventory - periodically document
- Information system documentation - how hardware, software and people connect
- Conduct risk assessment periodically - once is not enough

Administrative People

- HIPAA officer, security officer
- Define all office staff roles and access to EPHI
- Define process for granting and removing access to EPHI* (even for patients)
- Training people to policies

Administrative

- Business Associates Agreements - anyone who assists you in handling hardware, software or data must comply to security guidelines.
- See handout

Administrative Breaches

Data Loss

- Policy for reporting breaches
- EPHI back up plan
- Disaster recovery plan
- Implementation and testing
- Functioning during a disaster

Physical

- Facilities - entrances and exits (including windows)
- Staff offices
- Workstation locations - visible
- Data Centers
- Device and Media Controls

Technical

- Unique passwords and user names
- Automatic logoff
 - after inactivity, proximity badges
- Encryption of transmitted data
- Audit controls - track who accessed what and when

Data Integrity

- **HIPAA Standard:** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Digital signatures

Authentication

- Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
- Four common ways -
 1. Something a person knows - password
 2. Something a person has - smart card
 3. Biometric identification - fingerprint, facial recognition
 4. A combination of two of the above

Data in Transit

- Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
- Encrypt data when deemed appropriate

Policies and Procedures

- Must have documentation
- Maintain record for six years

CCHIT Security Requirements in EMRs examples

- Examples of how Certification feature requirements assure HIPAA compliance*
- Audit capabilities
- Role assignments
- Password rules
- Inactivity logouts
- Data Integrity
- Back up capabilities

*examples not inclusive of all features. See cchit.org for full listing.

Exhibits

- Exhibit 1 - Security Official Job Responsibilities
- Exhibit 2 - HIPAA Security Rule Standards Matrix and Risk Analysis
- Exhibit 3 - Audit Trails Policy & Procedures
- Exhibit 4 - Event Record
- Exhibit 5 - Policy for User Identification (User ID) and Authentication
- Exhibit 6 - Anti-Virus Policies and Procedures

Exhibits

- Exhibit 7 - Security Incident Report
- Exhibit 8 - Backup Policy and Procedure
- Exhibit 9 - Security Incident Policies and Procedures
- Exhibit 10 - Security Incident Log

Exhibits

- Exhibit 11 - Facility Maintenance Log
- Exhibit 12 - Contingency Policy and Procedure
- Exhibit 13 - Contingency Plan Steps
- Exhibit 14 - Listing Business Associates

Exhibits

- Exhibit 15 - Process for Determination of Business Associates that may have access to or work with EPHI
- Exhibit 16 - Business Associate Agreement

Web Sites

- HIPAA Security
<http://www.cms.hhs.gov/SecurityStandard/>
- CCHIT - www.cchit.org
- Specialty Web sites will have templates