Working with HIT Systems

Unit 7 Protecting Privacy, Security, and Confidentiality in HIT Systems

Objectives

By the end of this unit the student will be able to:

- Explain and illustrate privacy, security, and confidentiality in HIT settings.
- Identify common threats encountered when using HIT.
- Formulate strategies to minimize threats to privacy, security, and confidentiality in HIT systems.

Electronic Health Information Risks and Opportunities

- Access to electronic vs. paper records
- Public apprehension around digitization of health information
- Success of HIT systems depends on ensuring patient privacy
- Security can facilitate patient-centered care

Privacy, Confidentiality, Security Defined

- Privacy: patient is in control
- Confidentiality: only authorized individuals are allowed access
- Security: controls/safeguards that ensure confidentiality

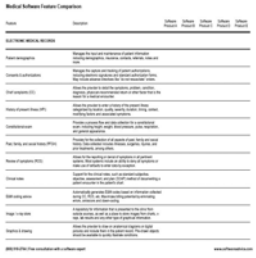
Security Management System Standards

- ISO 27001
- NIST 800-53
- HIPAA

Medicaid HIPAA Outreach Activities

HIPAA and PHI

- Health Insurance Portability and Accountability Act of 1996
- Privacy Rule (effective 2003)
- Security Rule (effective 2005)
- HITECH Act of 2009



Medical Software Feature Comparison

Types of Security Safeguards

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Administrative Safeguards

- Security Management Process
  - Risk Analysis
  - Risk Management
  - Sanction Policy
  - System Activity Review

Administrative Safeguards

- Assigned Security Responsibility
  - Security officer

Administrative Safeguards

- Workforce Security, Information Access Management
  - Who can and who cannot have access
  - Who determines who can have access and how
  - Employee turnover
  - Contractors
  - User roles

Administrative Safeguards

- Security Awareness and Training
  - Training
  - Security reminders
  - Log-in monitoring
  - Password management

Administrative Safeguards

- Security Incident Procedures
- Contcontingency Plan
  - Data backup
  - Disaster recovery
  - Emergency operation plan

Administrative Safeguards

- Evaluation
- Business Associate Agreements

Physical Safeguards

- Facility Access Controls

Physical Safeguards

- Workstation Use
- Workstation Security
- Device and Media Controls (e.g., media disposal, access to backup and storage media)

Physical Safeguards

- Device and Media Controls
  - media disposal
  - access to backup and storage media

Technical Safeguards

- Access Control
  - Unique user identification
  - Emergency access
  - Automatic logoff
  - Encryption/decryption

Technical Safeguards

- Audit Controls
- Integrity

Technical Safeguards

- Person or Entity Authentication
  - Password/Passphrase/PIN
  - Smart card/token/key
  - Biometrics
  - Two factor authentication

Technical Safeguards

- Transmission Security
  - Integrity controls
  - Encryption

Risk Analysis and Management

- Analysis
  - Gather data on potential threats and vulnerabilities
  - Assess current security measures
  - Determine likelihood, impact and level of risk
  - Identify needed security measures
- Management
  - Develop a plan for implementation
  - Evaluate and maintain security measures

Meaningful Use

- Criteria for meaningful use of EHRs related to privacy, security and confidentiality meant to align with HIPAA
- Emphasizes need to conduct a risk analysis
- Some specific requirements for EHR vendors

Summary

- Privacy, security, and confidentiality in HIT settings
- Common threats encountered when using HIT
- Strategies to minimize threats to privacy, security, and confidentiality in HIT systems.