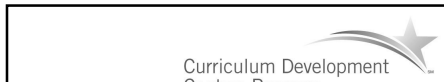


Awardee of The Office of the National Coordinator for Health Information Technology

Component 8
Installation and Maintenance of Health IT Systems

Unit 6a
System Security Procedures and Standards

This material was developed by Duke University, funded by the Department of Health and Human Services, Office of the National Coordinator for Health Information Technology under Award Number IU24OC000024.

What We'll Cover

- Regulatory requirements
  - HIPAA privacy and security rules
- Best practices
- Identify and assess protection measures
  - Access control
  - Firewalls
  - Intrusion detection
  - Encryption
  - Importance of user training

Security and Privacy

- Federal, state, and local laws govern access to and control of health record information, particularly:
  - Who can have access
  - What should be done to protect the data
  - How long the records should be kept
  - Whom to notify and what to do if a breach is discovered

Security and Privacy: HIPAA

- HIPAA = Health Insurance Portability and Accountability Act of 1996
  - Protected health information (ePHI) includes any health information that:
    - Explicitly identifies an individual
    - *Could reasonably be expected to allow* individual identification.
  - Excludes PHI in education records covered by Family Educational Rights and Privacy Act (FERPA), employment records.

Security and Privacy: HIPAA (cont'd)

- 18 identifiers recognized as providing identifiable links to individuals.
  - Name, address, ZIP code
  - Dates (birth dates, discharge dates, etc.)
  - Contact info, including email, web URLs
  - Social Security Number or record numbers
  - Account numbers of any sort
  - License number, license plates, ID numbers
  - Device identifiers, IP addresses
  - Full face photos, finger prints, recognizable markings

Security and Privacy (cont'd)

- State and local laws vary.
- Federal law tends to supersede state and local laws. Where overlap occurs, always choose the tightest constraint.
- Our lecture will focus on federal regulatory obligations.

What is HIPAA Privacy?

- Federal law governing privacy of patients' medical records and other health information maintained by covered entities including:
  - Health plans, including Veterans Health Administration, Medicare, and Medicaid
  - Most doctors & hospitals
  - Healthcare clearinghouses
- Gives patients access to records and significant control over use and disclosure.
- Compliance required since April 2003.

HIPAA Privacy Rule

- Privacy and security complaints
  - All investigated by Office of Civil Rights (OCR) of Dept. of Health and Human Services (HHS), as of 2009.
  - 54,562 complaints received (as of August 2010), of which 11,632 required corrective actions.
  - Steep fines for validated complaints.
  - Entities needing the most corrective actions:
    - Private health care practices
    - General hospitals
    - Pharmacies
    - Outpatient facilities
    - Group health plans

HIPAA Privacy Rule (cont'd)

- Violations investigated most often:
  1. Impermissible uses and disclosures of protected health information (ePHI)
  2. Lack of safeguards of ePHI
  3. Lack of patient access to their ePHI
  4. Uses or disclosures of more than the minimum necessary ePHI
  5. Complaints to the covered entity

HIPAA Security Rule

- Established standards for securing electronic protected health information (ePHI) created, received, maintained, or transmitted.
  - Delineated as “required” or “addressable”.
  - Designed to be flexible, scalable.
- By 2005, entities required to:
  - Ensure confidentiality, integrity, availability.
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information.
  - Protect against reasonably anticipated, impermissible uses or disclosures.
  - Ensure compliance by workforce.
- Works in tandem with Privacy Rule.

What is Required by HIPAA Security Rule?

- Categories:
  1. Administrative safeguards
  2. Physical safeguards
  3. Technical safeguards
  4. Organizational requirements

Common Security Breaches

According to the TCP/IP Core Networking Guide from Microsoft:

- Inside jobs, social engineering
- Brute force
- Eavesdropping, sniffing, snooping
- Data modification
- Identity spoofing
- Password-based attacks
- Denial of service attacks
- Man in the middle attacks
- Application layer attacks

Administrative Safeguards

- Address process of security management in your organization.
- Risk analysis
  - Evaluating likelihood and impact of potential risks to ePHI
  - Implementing appropriate security measures to address identified risks
  - Documenting security measures chosen, with rationale
  - Maintaining continuous, reasonable, appropriate protections
- Ongoing process, with regular reviews

Administrative Safeguards (cont'd)

- Designated security official
  - Responsible for developing and implementing security policies and procedures.
  - Knowledge of good HIPAA practices
  - Familiarity with established IT security standards
  - Ability to interface well with all levels of management and staff

Administrative Safeguards (cont'd)

- Policies & procedures for authorizing access to ePHI only when appropriate for one's role (role-based access).
  - Who gets access to ePHI data?
  - What level of access is needed?
  - Who is the agent authorizing the access?
  - Is this authorization adequately documented?
  - Is the access periodically reviewed?
  - Is there a process for rescinding access when no longer needed?

Administrative Safeguards (cont'd)

- Processes for appropriate authorization and supervision of workforce members who work with ePHI.
- Well-documented training of all workforce members in security policies and procedures
  - Appropriate sanctions against violators.

Physical Safeguards: Access

- Limit physical access to facilities, while ensuring that authorized access is allowed.
  - Server rooms where ePHI is stored
  - Work areas where ePHI is accessed
  - Back-up media storage potentially containing ePHI
- Inventory hardware and software.
  - Know where inventory is kept.
  - Know value of hardware, software, equipment.

Physical Safeguards: Access (cont'd)

- Policies and procedures for proper use of & access to workstations & electronic media, including transfer, removal, disposal, re-use.
  - Lock down publicly-accessible systems potentially containing ePHI.
  - Strong passwords (8-14 characters with variety of letters, symbols, numbers) changed regularly.
  - At least 256-bit encryption, especially for wireless, backups, & offsite data.
  - Media destroyed after being thoroughly wiped.

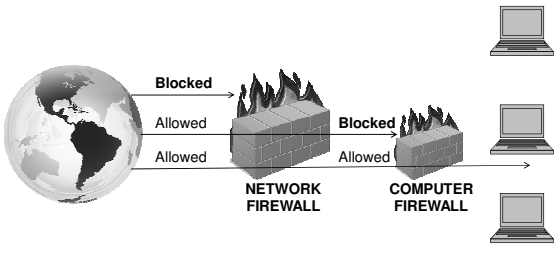
Technical Safeguards: Access Control

- Access controls, audit controls, integrity, person, user/entity authentication, transmission security
- Most effective: layered approach.
  - Multiple technologies employed concurrently.
- Adequate access controls include:
  - AD (Active Directory), LDAP (Lightweight Directory Access Protocol)
  - Vendor-specific controls usually part of EHR

Technical Safeguards: Firewall

- Inspects incoming network traffic; permits or denies access based on criteria.
- Hardware- or software-driven.
- Blocks ports through which intruders can gain access (e.g., port 80, which regulates web traffic).
- Most commonly placed on network perimeter (network-based) or network device (host-based).
- EHR will require certain ports to remain open.

Firewalls



Summary

- Protected health information (ePHI)
  - Strictly regulated by HIPAA and other government guidelines prohibiting unwanted, unauthorized access.
  - Should be protected using layered approach, including numerous, administrative, physical, and technical safeguards.
- Firewalls as first-level technical safeguard.

Reference

- Summary of the HIPAA Security Rule, US Department of Health & Human Services
  - http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
- "Common Types of Network Attacks" Microsoft Windows TCP/IP Core Networking Guide. Distributed Systems Guide, Windows 2000 Server
  - http://technet.microsoft.com/en-us/library/cc959354.aspx
- Strong Password Definition, Requirements, and Guidelines
  - http://ebenefitswebsites.com/home/sub1/faq/