Installation and Maintenance of Health IT Systems

Unit 6a

System Security Procedures and Standards

What We'll Cover…

- Identify the 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

Under HIPAA, protected health information (PHI) includes:

- any *individually identifiable* health information, as well as
- health information with data which could reasonably be expected to allow individual identification.

Security and Privacy

Federal, state, and local laws control access to and control of health record information. These laws govern:

- Who can have access
- What should be done to protect the data
- How long the records should be kept
- What to do if a breach is discovered

Security and Privacy

18 identifiers are recognized as providing identifiable links to individuals, including:

- Names, addresses, ZIP codes
- Dates (birth dates, discharge dates, etc.)
- Contact info, including email, web URLs
- Social Security Numbers or record numbers
- Account numbers of any sort
- License numbers, license plates, ID numbers
- Device identifiers, IP addresses
- Full face photos, finger prints, recognizable markings

Security and Privacy

- 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.

Common Types of Security Breaches

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

What is HIPAA Privacy?

- Federal law governing privacy of patients' medical records and other health information maintained by covered entities
- Covered entities include:
  - Health plans, including Veterans Health Administration, Medicare, and Medicaid
  - Most doctors & hospitals
  - Health care clearinghouses
- Compliance required since April 2003

HIPAA Privacy Rule

- Health and Human Services’ (HHS) Office of Civil Rights (OCR) investigates all Health Insurance Portability and Accountability Act (HIPAA) privacy and security complaints
  - 54,562 complaints received as of August 2010
- Filed against:
  - Private health care practices
  - General hospitals
  - Pharmacies
  - Outpatient facilities
  - Group health plans

HIPAA Privacy Rule

Compliance issues investigated most often:

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

HIPAA Security Rule

- Established standards for securing electronic protected health information (ePHI)
  - Ensure confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit
  - 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 their workforce

What is Required by HIPAA Security?

HIPAA Security requirements can be broken down into four categories:

- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Organizational requirements

Administrative Safeguards

- Address the “process” of security management in your organization
- Require a **risk analysis** be performed and steps taken to mitigate identified risks. This analysis includes:
  - Evaluating the likelihood and impact of potential risks to e-PHI
  - Implementing appropriate security measures to address the risks identified in the risk analysis
  - Documenting the chosen security measures and, where required, the rationale for adopting those measures
  - Maintaining continuous, reasonable, and appropriate security protections

Administrative Safeguards

- You must designate a security official responsible for developing and implementing security policies and procedures. This person should:
  - Have knowledge of good HIPAA practices and be familiar with established IT security standards.
  - Be able to interface well with all levels of management and staff.

Administrative Safeguards

- Require a covered entity to implement policies and procedures for authorizing access to ePHI only when such access is appropriate based on the user’s or recipient's role (role-based access).
- Can your policy address these questions?
  - 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 once it’s no longer needed?

Administrative Safeguards

- Must set up processes for appropriate authorization and supervision of workforce members who work with e-PHI.

- Must routinely train all workforce members regarding security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate Its policies and procedures.

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 your hardware and software.
  - Know where the inventory is kept.
  - Know the value of your hardware, software, equipment.

Physical Safeguards - Access

- Implement policies and procedures specifying proper use of and access to workstations and electronic media, including its transfer, removal, disposal, and re-use.
  - Lock down publicly-accessible systems potentially containing ePHI.
  - Use strong passwords (8-14 characters with a variety of letters, symbols, and numbers) that are changed regularly.
  - Encrypt electronic media using 256-bit encryption, especially for wireless, backups, and offsite data.
  - ePHI media should be destroyed after being thoroughly wiped.

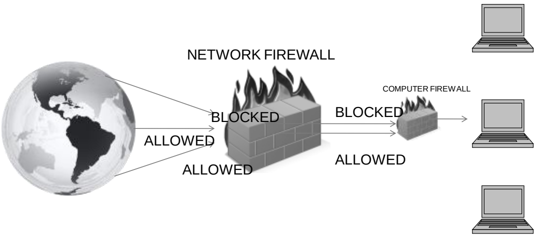
Technical Safeguards - Access Control

- Addresses access controls, audit controls, integrity, person, or entity authentication and transmission security.
- HIPAA security rules require measures to guard against unauthorized access. Adequate access controls include:
  - Active Directory / LDAP
  - Vendor-specific controls

Technical Safeguards - Access Control

- Firewall
  - Inspects incoming network traffic and permits or denies access based on a set of criteria.
  - May be hardware or software driven.
  - Blocks ports through which an intruder can gain access.
  - Is most commonly placed on the network perimeter (network-based) or on a network device (host-based).

Firewalls


NETWORK FIREWALL
COMPUTER FIREWALL
BLOCKED
ALLOWED
ALLOWED
BLOCKED
ALLOWED