NURS 737: Concepts in Nursing Informatics
Module 2, Subtopic 3

Privacy, Confidentiality, Security, and HIPAA

Privacy, Confidentiality, & Security

Definitions

- Privacy - freedom from unauthorized intrusion
- Confidentiality - the condition of being hidden or concealed
- Security - measures taken to guard against espionage or sabotage, crime, attack, or escape

Privacy, Confidentiality, & Security

- Are computer records safer than paper?
- How vulnerable is electronically-stored, individually identifiable health information (IIHI or PHI)?
- Consider the scenario in the next slide as evidence of its vulnerability:

Scenario

A university hospital information systems specialist inadvertently placed a ten-megabyte patient scheduling log on the hospital's intranet website. Within this log were the names, addresses, social security numbers, employer information, diagnoses, and treatment plans of hundreds of patients.

The Health Insurance Portability and Accountability Act (HIPAA)

- The HIPAA law has evolved over time.
- The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191)
  - Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the Department of Health and Human Services (HHS) to adopt **national standards for electronic health care transactions and national identifiers for providers, health plans, and employers**.
  - The AS provisions also address the **Security and Privacy of health data.**

(http://www.cms.gov/HIPAAGenInfo/01_Overview.asp#TopOfPage)

The Health Insurance Portability and Accountability Act (HIPAA)

- Under the Affordable Care Act of 2010, provisions to HIPAA of 1996 further increase use of electronic data interchange and include requirements to adopt:
  - operating rules for each of the HIPAA covered transactions
  - a unique, standard Health Plan Identifier (HPID)
  - standard and operating rules for electronic funds transfer (EFT), electronic remittance advice (RA), and claims attachments.
- In addition, health plans will be required to certify their compliance.

(http://www.cms.gov/HIPAAGenInfo/01_Overview.asp#TopOfPage)

HIPAA Omnibus Rule

- Much has changed in health care since HIPAA was enacted over fifteen years ago. The new rule will help protect patient privacy and safeguard patients' health information in an ever expanding digital age.

(http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html)

Administrative Simplification

The purpose of this law is to “mandate new security standards to protect an individual’s health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses, and health plans.”

Administrative Simplification

- Electronic transactions and code sets standards requirements
- Privacy requirements
- Security requirements
- National identifier requirements

HIPAA

(https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/TransactionCodeSetsStands/index.html?redirect=/TransactionCodeSetsStands/)

- Transaction Standards (ANSI X12N)
  - Administrative (claims, eligibility, benefits)
- Code Sets
  - ICD-9 /ICD-10 (As of October 1, 2015), NDC (National Drug Codes), CPT-4 (Physicians Procedures), HCPCS (Ancillary Services/Procedures)
- Unique Health Identifiers
  - Patients
  - Providers
  - Healthcare Plans
- Security provisions
- E-signature

How HIPAA Affects Whom

- Employer Identifier gives a unique code to your employer for Medicare/Medicaid/FICA purposes
- Privacy and Confidentiality Standards and Security Standards affect the entire healthcare continuum
- Transactions and Code Sets Standards require specific coding criteria for all electronic transactions with CMS

Goal of Privacy Rules

"…to ensure that protections for patient privacy are implemented in a manner that maximizes privacy while not compromising either availability or the quality of medical care"

Privacy Rules

- Marketing
  - PHI cannot be sold to third parties without prior consent
- Consent and Notice
  - Requires providers to notify patients of their rights and make a good faith effort to secure written acknowledgement
  - Allows disclosure of PHI for fraud and abuse investigations

Privacy Rules

- Uses and Disclosures for FDA
  - Allows disclosure for certain purposes without consent
- Incidental Use and Disclosure
  - Allows disclosure of minimum necessary PHI with safeguards applied
- Authorization
  - Individual authorizations not required for routine uses

Privacy Rules

- Minimum Necessary Standards
  - Permits disclosure of ONLY the data necessary for the prescribed purpose
- Parents and Minors
  - Governed by state laws
- Business Associates
  - Requires new contracts be written that satisfy the minimum necessary provisions within one year

Security & Confidentiality Concerns for the INS

- Audit trails
- Access control (PINS, passcards, etc.)
- The biggest threat is inappropriate use by unauthorized users
- Way to attack is to “increase accountability”

Security & Confidentiality Concerns for the INS

- The four A's
  - Authentication
  - Access
  - Audit train analysis
  - Accountability
- HIPAA or not, these should guide your policy
- Lock it up versus make it available
- Employee behavior must be addressed
- Strong policy on inappropriate access

Curriculum Development Centers Program

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

System Security

(selected components)

Adapted From ONC Lecture Slides

Installation and Maintenance of Health IT Systems

System Security Procedures and Standards

(Comp8_Unit6a)

This material Comp8 _Unit6a 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.

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.

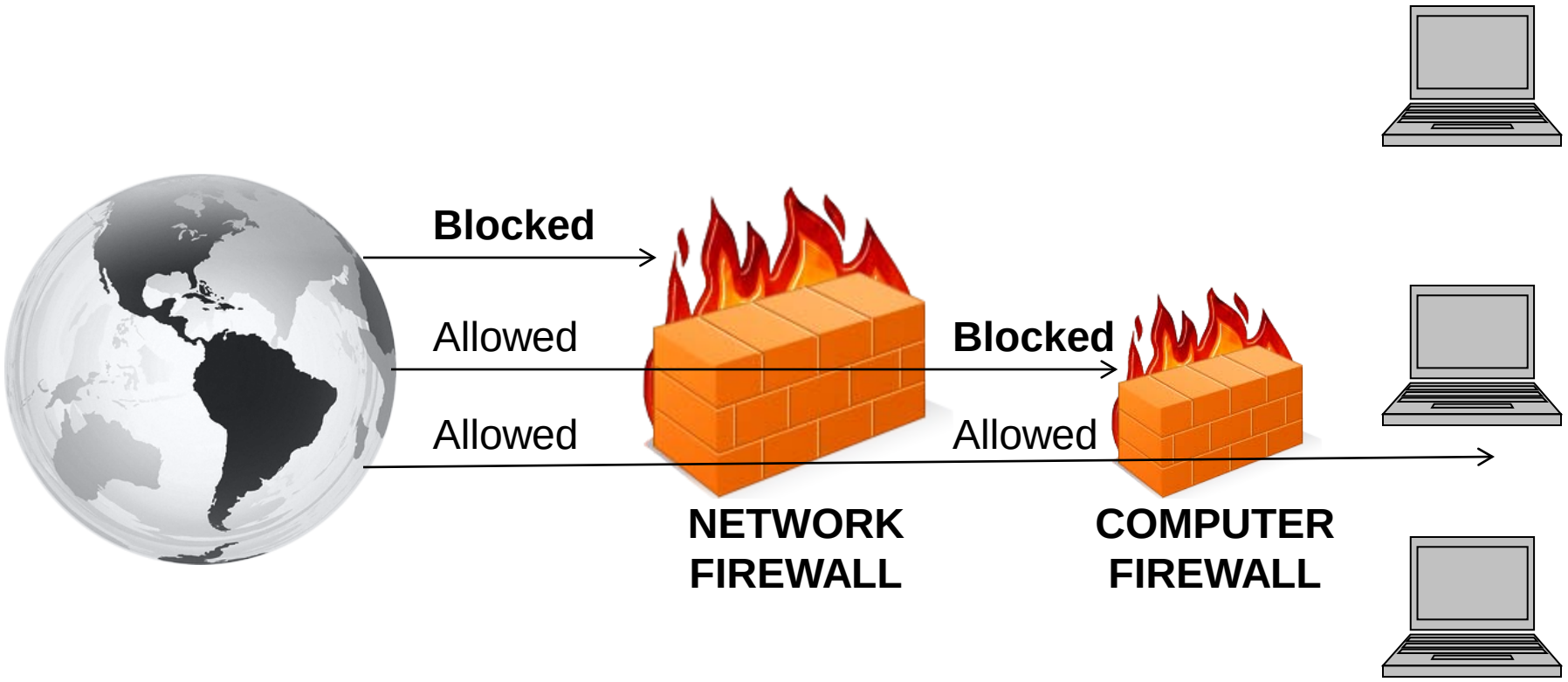
Technical Safeguards: Access Control

- 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


Blocked
Allowed
Allowed
Blocked
Allowed
NETWORK FIREWALL
COMPUTER FIREWALL

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/

Recent Changes in HIPAA

- New HIPAA guidance reiterates patients' right to access health information clarifies appropriate fees for copies
  - http://www.hhs.gov/blog/2016/02/25/new-hipaa-guidance-accessing-health-information-fees-copies.html
- Obama Administration Modifies HIPAA to Strengthen the Firearm Background Check System
  - http://www.hhs.gov/blog/2016/01/04/obama-administration-modifies-hipaa.html