Week 9: Health Information Privacy and Security

Dr. Ranyah Aldekhyyel
Assistant Professor in Health Informatics
Medical Education Department
Medical Informatics &e-learning Unit

email: raldekhyyel@ksu.edu.sa

Acknowledgment:

This presentation is adopted from the Book

“Health Informatics Practical Guide- Seventh Edition”©

Chapter 10: Health Information Privacy and Security by John Rasmusen

INFORMATICSEDUCATION

Advancing Health Informatics Education

Learning Objectives

After this lecture, you should be able to:

* Explain the importance of confidentiality, integrity, and availability
* Describe the regulatory environment and how it drives information privacy and security programs within the health care industry
* Recognize the importance of data security and privacy as related to public perception, particularly regarding data breach and loss
* Identify different types of threat actors and their motivations
* Identify different types of controls used and how they are used to protect information
* Describe emerging risks and how they impact the health care sector

Three Pillars of Data Security

Pillar 1: confidentiality

- prevention of data loss
- category most easily identified with HIPAA privacy and security within healthcare environments
- usernames, passwords, and encryption are common measures implemented to ensure confidentiality

Pillar 2: availability

- system and network accessibility
- focuses on power loss or network connectivity outages
- Loss of availability may be attributed to natural or accidental disasters , but also refer to man-made scenarios
- backup generators, continuity of operations planning and peripheral network security equipment are used to maintain availability

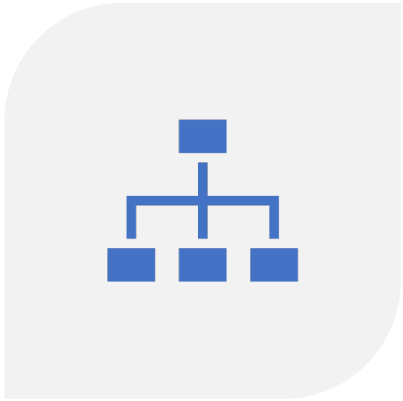
Pillar 3: integrity

- describes trustworthiness and permanence of data, an assurance that the lab results or personal medical history of a patient is not modifiable by unauthorized entities or corrupted by a poorly designed process
- Database best practices, data loss solutions, and data backup and archival tools are implemented to prevent data manipulation, corruption, or loss

Defense in Depth for Healthcare

* Data must be classified to determine its risk
* Healthcare organizations must develop a set of controls to protect confidentiality, integrity and availability of data
* One layer of defense is not likely to be adequate
* Healthcare organizations will need technical, administrative and physical safeguards

Types of Safeguards



ADMINISTRATIVE

PHYSICAL

TECHNICAL

Administrative Safeguards

* **Administrative Safeguards**
  * Security management processes to reduce risks and vulnerabilities
  * Security personnel responsible for developing and implementing security policies
  * Information access management-minimum access to perform duties
  * Workforce training and management
  * Background checks, drug screens, etc. for new employees
  * Evaluation of security policies and procedures

Physical Safeguards

* **Physical Safeguards**
  * Limit physical access to facilities
  * Workstation and device security policies and procedures covering transfer, removal, disposal, and re-use of electronic media
  * Badge with photo

Technical Safeguards

- **Technical Safeguards**
  - Access control that restricts access to authorized personnel
  - Audit controls for hardware, software, and transactions
  - Integrity controls to ensure data is not altered or destroyed
  - Transmission security to protect against unauthorized access to data transmitted on networks and via email
  - Unique usernames and passwords, encrypted software, anti-virus software, secure email, firewalls, etc.

Healthcare Regulatory Environment

* Health Insurance Portability & Accountability Act (HIPAA - 1996)
  * Laid ground work for privacy and security measures in healthcare . Initial intent was to cover patients who switched physicians or insurers (portability)
* Next important Act was the American Recovery and Reinvestment Act (ARRA - 2209) & HITECH Act that imposed new requirements for breach notification and stiffer penalties

Covered Entities or Those Who Must Follow HIPAA Privacy Rule

* Health Plans: Health insurers, HMOs, Company health plans, Government programs such as Medicare and Medicaid
* Health Care Providers who conduct business electronically: Most doctors, Clinics, Hospitals, Psychologists, Chiropractors, Nursing homes, Pharmacies, Dentists

Saudi Legislation

- The Saudi Health Information Exchange Policies ('the SHIE Policies'), published by the Ministry of Health.
- In line with Vision 2030, the MoH published a suite of policies relating to the Saudi Health Information Exchange ('SHIE') initiative (also referred to as the Saudi eHealth Exchange 'SeHE')
- broadly aimed at the use of health information, including patient data, in the context of the increased adoption of technology and digitalization in the health system.
- The policies provide a clearer understanding of what the MoH expects in terms of the use of data in a healthcare context.

Saudi Guidelines

- The Patient's Bill of Rights and Responsibilities ('the Patient's Bill') (MOH bill), as an example
- The Patient's Bill sets out patients' main rights and duties whenever receiving health services from the relevant health facilities (a health facility is defined by the Patient's Bill as the agency affiliated to the MoH or operating under its supervision and providing health services to patients; whether a clinic, health center, infirmary, hospital, or laboratory).
- One of these essential rights is the patient's right to confidentiality and security.

Covered Entities: Patient Rights

* Request and receive a copy of their health records
* Request an amendment to their health record
* Receive a notice that discusses how health information may be used and shared, the Notice of Privacy Practices
* Request a restriction on the use and disclosure of their health information
* Receive a copy of their "*accounting of disclosures*"
* Restrict disclosure of the health information to an insurer if the encounter is paid for out of pocket
* File a complaint with a provider, health insurer, and/or organization if patient rights are being denied or health information is not being protected.

Protected Health Information (PHI)

* Individually identifiable health information:
  * Information created by a covered entity
  * *And "relates to the past, present, or future physical or mental health or condition of an individual"*
  * *Or* identifies the individual or there is a reasonable basis to believe that the individual can be identified from the information.

HIPAA

* Protections apply to all personal health information (PHI), whether in hard copy records, electronic personal health information (ePHI) stored on computing systems, or even verbal discussions between medical professionals
* Covered entities must put safeguards in place to ensure data is not compromised, and that it is only used for the intended purpose
* The HIPAA rules are not designed to and should not impede the *treatment* of patients

Privacy Rule Mandates Removal of 18 Identifiers

* Names
* All geographic subdivisions smaller than a state
* All elements of dates (except year)
* Telephone numbers
* Facsimile numbers
* Electronic mail addresses
* Social security numbers
* Medical record numbers
* Health plan beneficiary numbers
* Account numbers
* Certificate/license numbers
* Vehicle identifiers and serial numbers, including license plate numbers
* Device identifiers and serial numbers
* Web universal resource locators (URLs)
* Internet protocol (IP) address numbers
* Biometric identifiers, including fingerprints and voiceprints
* Full-face photographic images and any comparable images
* Any other unique identifying number, characteristic, or code

Permitted Uses and Disclosures of Patient Data

- To the individual
- For treatment, payment or health care operations
- Uses and disclosures with opportunity to agree or object
  - Facility directories
  - For notification and other purposes
- Incidental use and disclosure
- Public interest and benefit activities
  - Required by law
  - Public health activities
- Victims of abuse, neglect or domestic violence
- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement purposes
- Decedents
- Cadaveric organ, eye, or tissue donation
- Research
- Serious threat to health or safety
- Essential government functions
- Workers' compensation

Administrative Requirements for the Privacy Rule

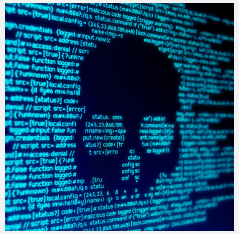
* Develop and implement written privacy policies and procedures
* Designate a privacy official
* Workforce training and management
* Mitigation strategy for privacy breaches
* Data safeguards - administrative, technical, and physical
* Designate a complaint official and procedure to file complaints
* Establish retaliation and waiver policies and restrictions
* Documentation and record retention - six years
* Fully-insured group health plan exception

Organizational Roles

* Policy regarding information security practices is often set by chief information officers (CIOs), chief technology officers (CTOs), information technology (IT) directors or similar; often with input from chief medical informatics officers (CMIOs), HIPAA compliance officers, or the like
* Depending on resources, the information technology teams may consist of network, system administration, security and data personnel, or could be the very same technical staff relied upon for all office or clinic IT needs

Threat Actors

INSIDERS



HACKIVISTS

ORGANIZED CRIME

Types of Attacks

* Social Engineering: most common
  * Phishing: via email or text messaging
  * Shoulder surfing: attacker looks over the shoulder
  * Tailgating: attacker uses someone else's ID
  * Free software: USB drive is found and plugged into a computer, introducing a virus

Types of Attacks

* Denial of Service (DOS): website is flooded with traffic, shutting it down
* Brute Force: random credential are rapidly thrown at website hoping to gain access
* Doxing: gathers info about a victim and publishes that to harass or embarrass the individual.

Security Breaches and Attacks

* Identity theft on the rise
* Physical Theft
  * Stolen laptops, computers, storage devices and servers
* The HHS website lists all of the reported data breaches affecting over 500 users. The site lists the covered entity, the number of breach victims, the type of breach and the location of data (laptop, server, paper, etc.)
* Breaches: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Threat Countermeasures
Authentication &Identity Management

* Accomplished with photo identification, biometrics, smart card technologies, tokens, and the old standard; user name and password
* Basic Authentication may vary depending on sensitivity of data, the capabilities of the systems, resource constraints - both technical and monetary, and the frequency of access
* Methods rely on what is known as two or multi-factor authentication: something one knows, something one has, or something that one is

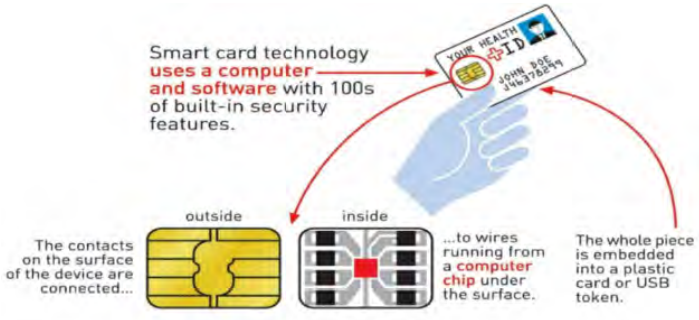
Authentication and Identity Management

* Basic authentication:
  * Username and password combination still employed by a majority of users today, combining two things that a user knows
  * Another option is utilizing a grid card, smart card, USB token, one time password (OTP) token, or OTP service in combination with something a user knows, such as a passphrase or PIN

Authentication and Identity Management

* Single Sign On (SSO)
  * One set of credentials to easily access many of the resources one uses every day securely; example is Google
* Smart Cards: Used in Healthcare in many countries
  * Vital information with a self-contained processor and memory
  * Low cost, ease of use, portability and durability, and ability to support multiple applications
  * Capable of encrypted patient information, biometric signatures and personal identification (PIN)
  * Drawbacks: lack of standardization and positive identification

Smart Cards in Healthcare



Authentication and Identity Management

* Biometric Authentication
  * When combined with passphrases or the tokens, cards, and OTP solutions discussed previously, a two or multi-factor authentication solution can be employed
  * Physical user identifiers: fingerprint, retinal scan, voice imprint

Theft Countermeasures

- Theft Countermeasures
  - Render data unusable to thieves
    - Encryption standards such as FIPS 140-2
    - Hardware and software encryption techniques
    - See encrypted USB device to the right

Conclusions

* Security of healthcare data is critical for future success of HIT
* Saudi laws and guidelines supplement the administrative, physical and technical safeguards implemented by HIPAA
* Security measures will continue to improve but so will the efforts of hackers and criminals who seek access to healthcare record data and identity theft