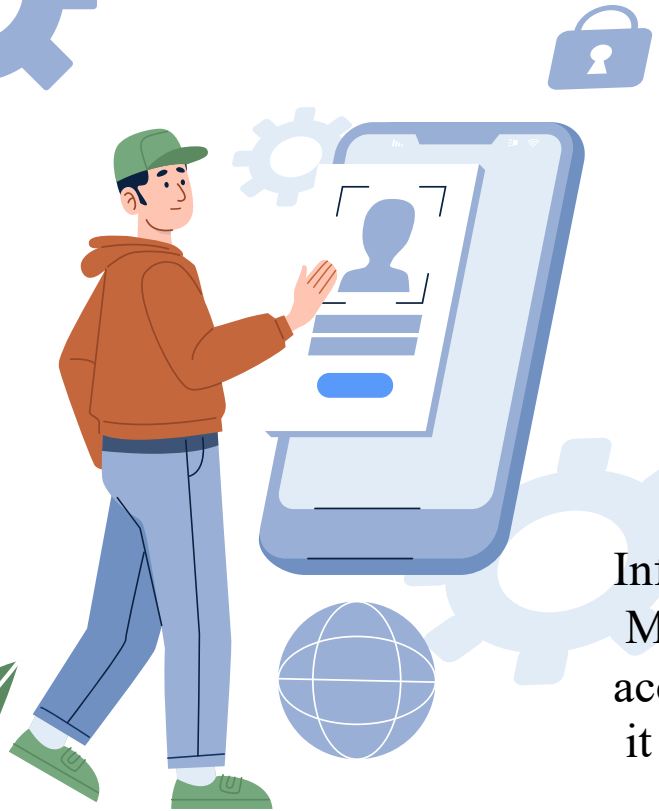
Electronic Health Records

Healthcare Security & Privacy Lecture: 5 & 6

M.Sc. Qusai Al-Durrah

01
What is Information security?



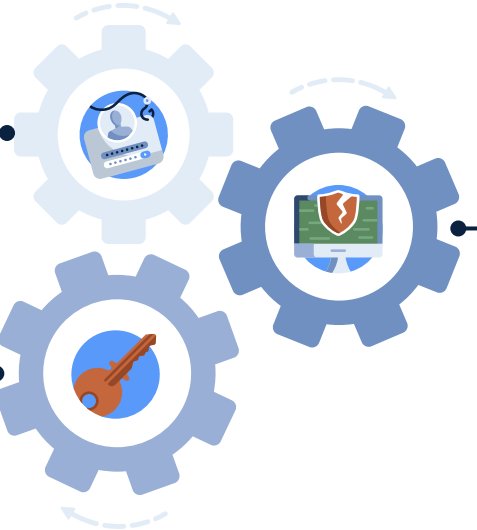
Information security is the protection of information from unauthorized access, use, disclosure or destruction through various means. This includes, but is not exclusive to, electronic data.

Information can include personal records as well as Medical data and businesses data. It may be stored and accessed using computers or in written records but it must be kept safe wherever it is located.

Principles of security

Confidentiality

Integrity



Availability

Principles of security

Confidentiality

is a set of rules that prevents sensitive information from being disclosed to unauthorized people, resources and processes. Methods to ensure confidentiality include data encryption, identity proofing and two factor authentication.

Integrity

ensures that system information or processes are protected from intentional or accidental modification. One way to ensure integrity is to use a hash function or checksum.

Availability

means that authorized users are able to access systems and data when and where needed are not. This can be achieved by maintaining equipment, performing hardware repairs, keeping operating systems and software up to date, and creating backups.

Principles of security

The main **function** of cyber security is to protect both the devices we use (computer Laptops smartphones etc.) and the data we access from malicious attacks, damage or misuse.

Cyber security A form of data protection The information that protected may include:

- Private and personal information.
- Sensitive or private information about employees clients patients or Customers.
- Confidential business integration
- Intellectual property.

02

Passive and Active Attacks

Cybersecurity Infographics

Passive Attack: Attempts to learn or make use of information from the system but does not affect system resources.

- Goal of attacker is to obtain information that is being transmitted

Active Attack: Attempts to alter system resources or affect their operation

- Goal of attacker is to steal data or changes it

Types of security Attacks

Types of security Attacks

Phishing

Malware

Virus

Worms

Trojan

Types of security Attacks

Phishing: Phishing attackers pretend to be a trustworthy party, usually through an email they send out.

Malware: Malware is short for malicious software and is designed to disrupt or damage data, software or hardware. Often, this means your device will no longer work as it should do.

- The attacker can install the malware onto your device using a variety of methods.
- All of them rely on you being tricked into downloading software for example:
- By clicking on an **unsafe link** or **attachment in an email** you may unknowingly download the malware.
- The malware may be attached to **a link on a website** which automatically downloads when you click on it

Types of security Attacks

Virus: is a type of malware that when you download it copies itself onto parts of data. computer applications or crucial parts of a computer's hard disk.

Worms: are similar to viruses in that they are also a type of malware that makes copies of itself to spread between devices.

Trojan: A Trojan is another type of malware that can damage your device. It is named after the wooden horse that the Greeks hid inside to infiltrate and attack the city of Troy.

03

Healthcare Security & privacy

Security in Healthcare

- 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**

Security in Healthcare

Administrative Safeguards

* Responsible for developing and implementing security policies
* Workforce training and management
* Evaluation of security policies and procedures

Physical Safeguards

* Limit physical access to facilities
* Procedures covering transfer, removal, disposal, and re-use of electronic media

Security in Healthcare

Technical Safeguards

* Access control that restricts access to authorized personnel
* 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
* Secure software and technologies

04

Protected Health Information PHI

Protecting personal Health Information

- Protections apply to all personal health information (PHI), whether in hard copy records, electronic personal health information (ePHI) stored on computing systems, or even discussions between medical professionals

- Covered entities must put safeguards in place to ensure data is not at risk

- The Privacy and security rules should not obstruct the *treatment* of patients

The Legal and Regulatory Context for EHRs

Electronic Health Records are among the most legally sensitive data systems in existence. Because EHRs contain **Protected Health Information (PHI)** and its electronic form **ePHI** — a combination of clinical data and personal identifiers — they are subject to a robust framework of federal and state regulations designed to safeguard patients and providers alike.

Privacy

Controls *who* may use or disclose PHI, and under what conditions — limiting access to authorized, need-to-know individuals.

Security

Protects ePHI against unauthorized access, use, disclosure, alteration, and destruction through technical and administrative safeguards.

Accountability

Requires the ability to trace every action taken on a record — *who* accessed it, *what* changed, and *when* — creating a defensible audit trail.

These three pillars translate directly into system-level controls: **authentication**, **authorization**, **audit logging**, **data retention policies**, and **breach response procedures**. Understanding this legal foundation is essential before designing or managing any EHR database environment.

Legal Process and the Electronic Health Record

In Health IT, "legal process" refers to the **operational workflows** governing how EHR data is requested, accessed, changed, disclosed, and retained. Every action taken on a patient record carries legal weight.

Authorization & Access Control

Define precisely **who** can access which EHR modules and functions. Role-based access control (RBAC) ensures clinicians, billing staff, and administrators each see only what their role requires — nothing more.

Consent & Permitted Disclosure

Patient data may flow freely for **treatment, payment, and operations (TPO)**. All other disclosures — to insurers, researchers, or third parties — require documented patient consent or a specific legal authorization.

Documentation Integrity

Records must be **trustworthy and tamper-evident**. Amendments are permitted, but original entries must be preserved. Silent changes — overwriting data without a trace — are a legal and ethical violation.

Audit Trail

Every view, edit, export, and disclosure must be logged with **who, what, and when**. Audit logs serve as legal evidence and are the foundation of accountability in any EHR system.

Retention & Disclosure Handling

Records must be retained for legally mandated periods (often 6–10 years). Requests for records must be fulfilled within defined timeframes, copies provided as permitted, and all disclosures formally logged.

From Legal Requirements to Database Design

Every legal and regulatory obligation has a **direct technical counterpart** in a relational database environment like SQL Server Management Studio (SSMS). If your database design cannot satisfy these mappings, you are failing your legal obligations — and putting patient data at risk.

Confidentiality

SQL logins, database users, and roles enforce **least privilege** — users access only the data their role requires. No exceptions.

Integrity

Primary keys, foreign keys, and constraints prevent invalid data. Controlled UPDATE procedures and **change history tables** preserve original records.

Availability

Regular **backups, maintenance plans, and disaster recovery** strategies ensure data is accessible when clinicians and patients need it.

Accountability

Audit tables capture **who, when, what action, old value, and new value** for every significant change — the database equivalent of a legal evidence trail.

privacy in Healthcare

Privacy Rules in Healthcare

2- Telephone numbers
Electronic mail addresses

4- Biometric identifiers, including fingerprints and voiceprints



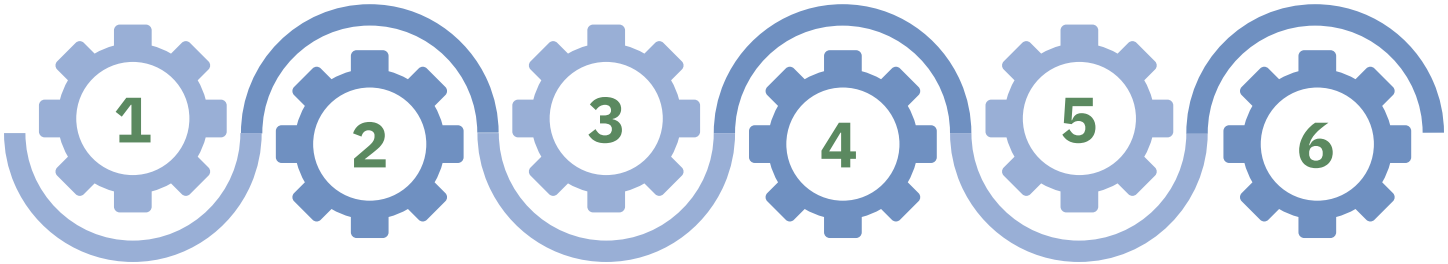


1- Names and All elements of dates

3- gov. ID numbers

5- Any other unique identifying number, characteristic, or code

Patient Rights



1. Request and receive a copy of their health records
2. Request changes to their health record
3. Receive a notice that discusses how health information may be used and shared
4. Request a restriction on the use and disclosure of their health information

Thanks!

Do you have any questions?