Introduction to Medical Informatics

Healthcare Security &
Privacy Lecture: 6 & 7

M.Sc. Qusai Al-Durrah

01
What is Information security?
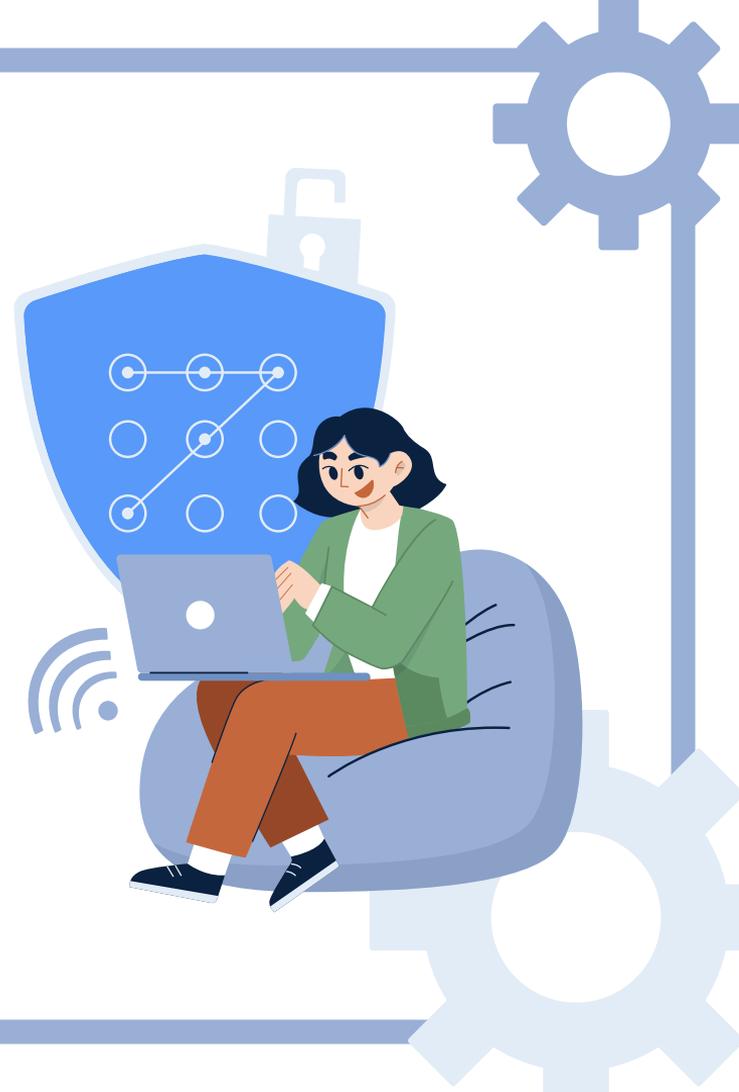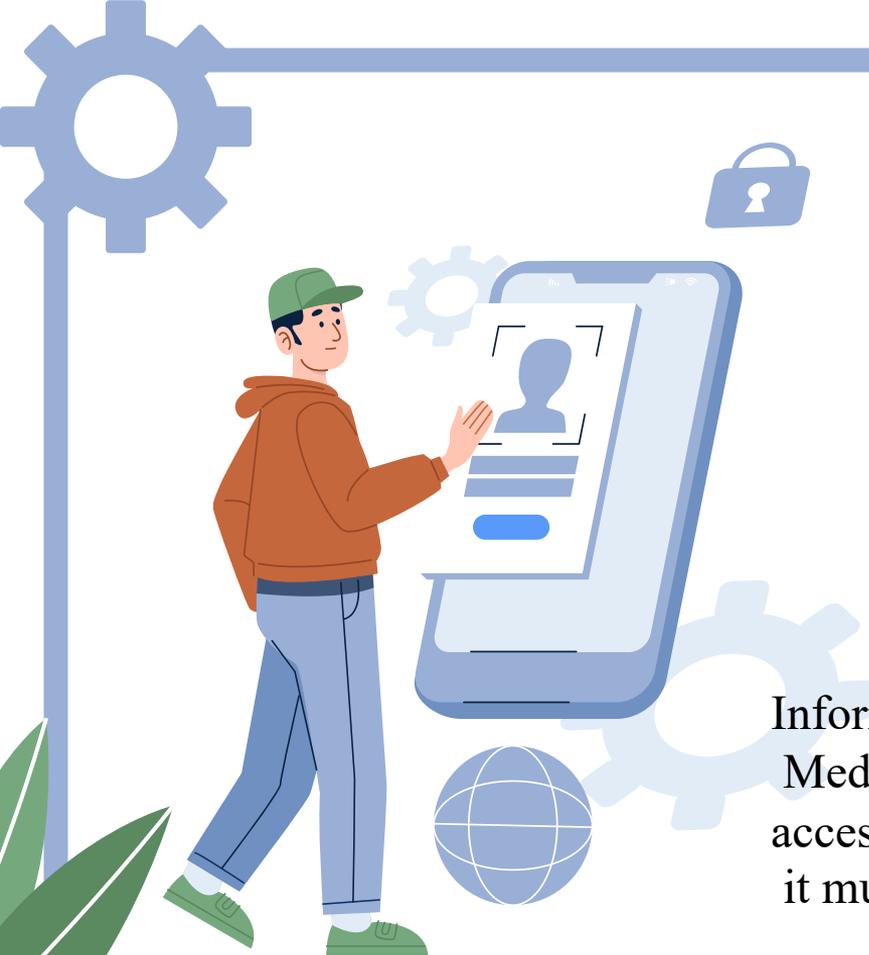
Information security is the protection of information from unauthorized access, use, disclosure or destruction through various means. This includes, but is not exclusive to, electronic data.
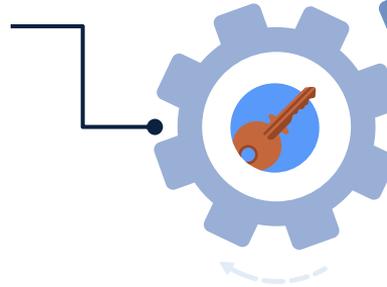
Information can include personal records as well as Medical data and businesses data. It may be stored and accessed using computers or in written records but it must be kept safe wherever it is located.

Principles of security
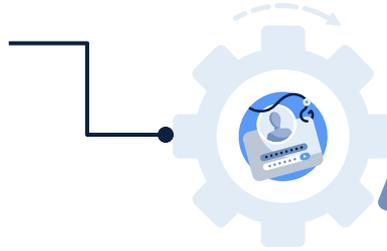
Confidentiality

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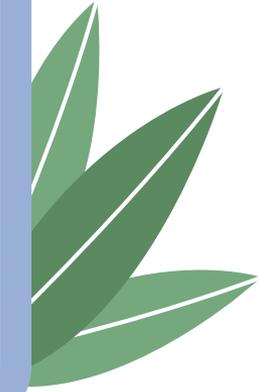
Cyber security A form of data protection The information that protected may include:

o Private and personal information.
o Sensitive or private information about employees clients patients or Customers.
o Confidential business integration
o Intellectual property.
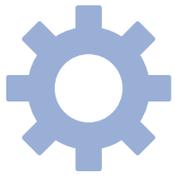
02

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.

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

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

o   Goal of attacker is to steal data or changes it

Types of security
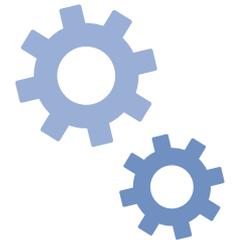Attacks

Types of security Attacks

Phishing

Malware
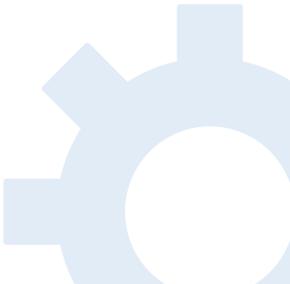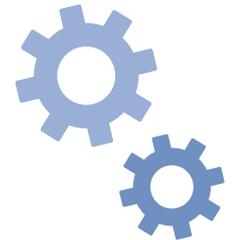
Virus

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.

- o The attacker can install the malware onto your device using a variety of methods.
- o 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.
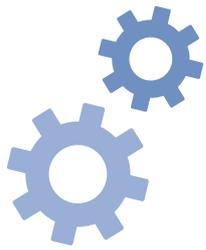
Trojan: A Trojan is another type of malware that can damage your device. It is named after the wooden horse that the Greeks hid inside to infiltrate and attack the city of Troy.
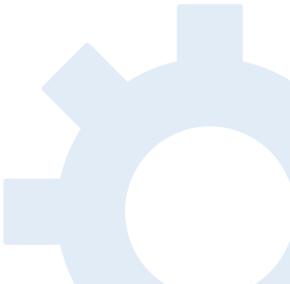
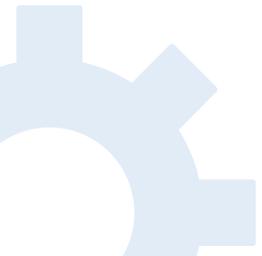# 03

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**
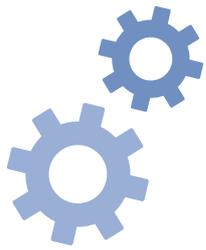
Security in Healthcare

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
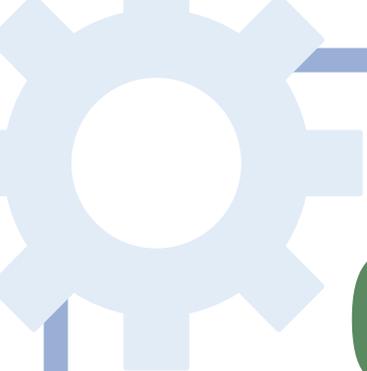
Security in Healthcare

Technical Safeguards
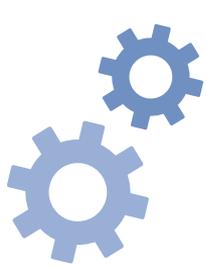
* Access control that restricts access to authorized personnel
* Integrity controls to ensure data is not altered or destroyed
* Transmission security to protect against unauthorized access to data transmitted on networks and via email
* Secure software and technologies

04

Protected Health Information (PHI)

Protected Health Information (PHI)

• 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

privacy in Healthcare
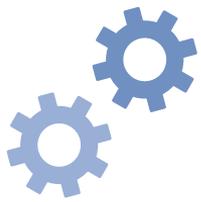
Privacy Rules in Healthcare

2- Telephone numbers
Electronic mail addresses

4- Biometric identifiers, including
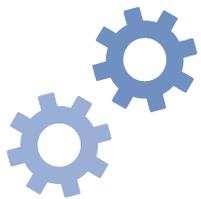fingerprints and voiceprints
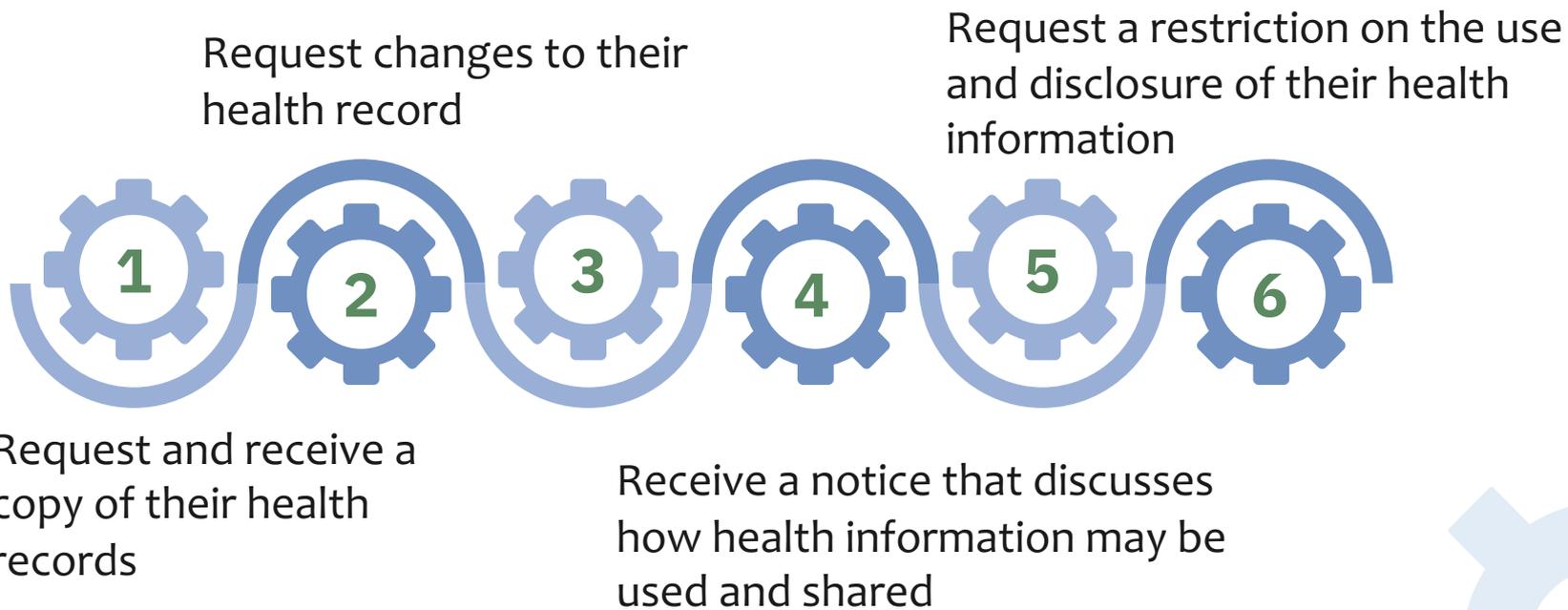
1- Names and All
elements of dates

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 Receive a notice that discusses how health information may be used and shared

5 Request a restriction on the use and disclosure of their health information

6

Thanks!

Do you have any questions?