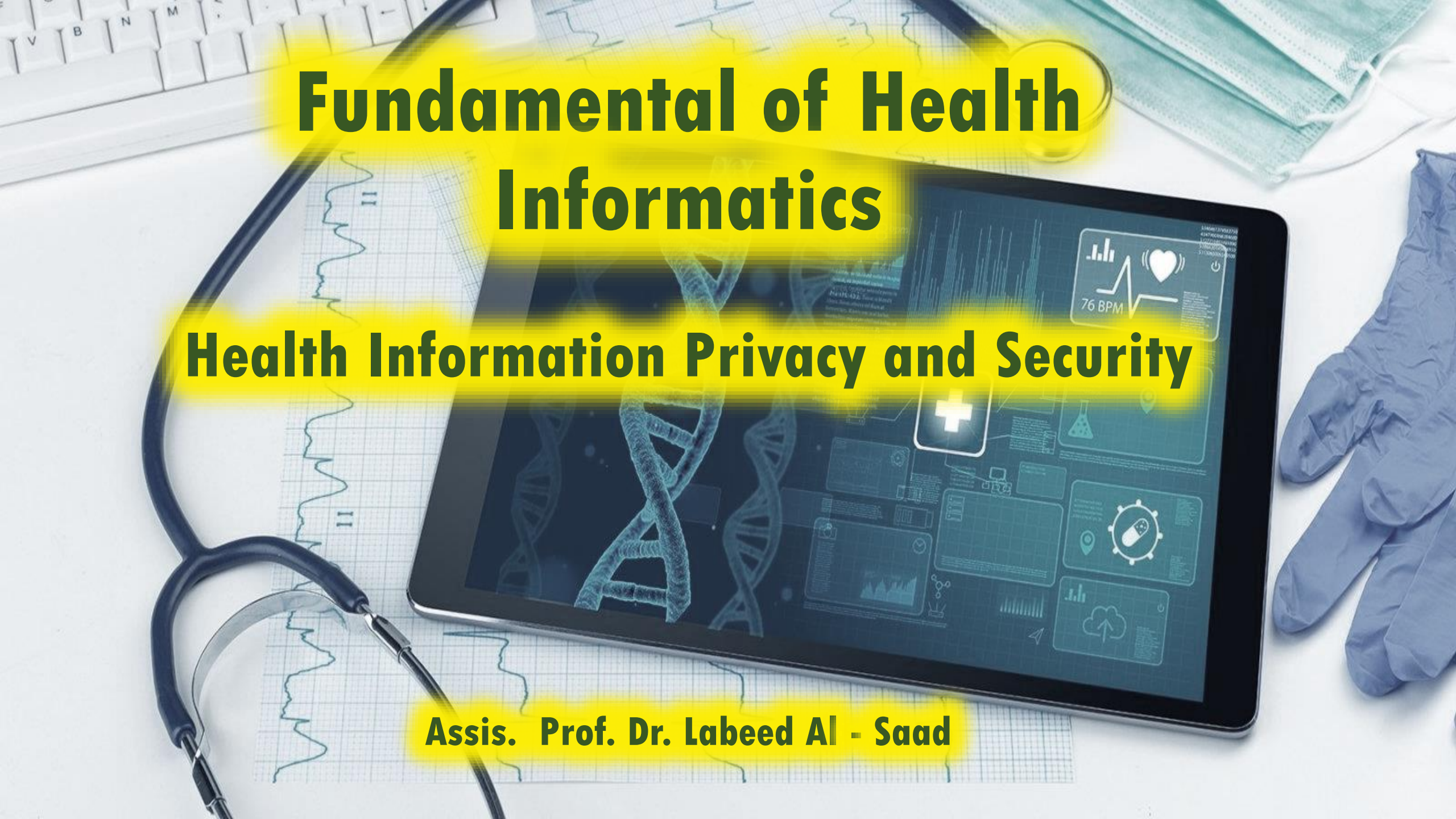
# Fundamental of Health Informatics

## Health Information Privacy and Security




Assis. Prof. Dr. Labeed Al - Saad

# The objectives

- Understanding Privacy and Confidentiality
- HIPAA (Health Insurance Portability and Accountability Act).
- Security Measures for Health Information.
- Data Breach Prevention and Response.
- Personalized Care.
- Patient Consent and Authorization.
- Interoperability and Health Information Exchange.
- Emerging Technologies and Privacy Challenges.
- Case Studies and Practical Scenarios.

# Understanding Privacy and Confidentiality

## Privacy vs. Confidentiality

- Privacy: A broader concept encompassing a patient's right to control their health information and decide who has access to it.
- Confidentiality: The specific duty of healthcare professionals and institutions to keep patient information secret and not disclose it without permission.

# Understanding Privacy and Confidentiality

## Legal and Ethical Obligations

- Laws like HIPAA (Health Insurance Portability and Accountability Act) mandate protecting patient privacy (PHI - Protected Health Information).
- Ethical codes for healthcare professions emphasize confidentiality and building trust with patients.

## Critical Scenarios for Confidentiality

- Sensitive diagnoses: HIV/AIDS, mental health conditions, genetic diseases.
- Conditions with potential social stigma or discrimination.
- Information that could endanger a patient's safety or well-being.

# HIPAA (Health Insurance Portability and Accountability Act)

The Health Insurance Portability and Accountability Act (HIPAA) is a cornerstone of patient health information privacy and security in the United States. It dictates how healthcare providers handle protected health information (PHI), impacting various aspects of healthcare practices.

Key HIPAA Rules:

Privacy Rule: Defines how PHI can be used, disclosed, and accessed by patients and authorized individuals. Patients have rights to request access, amend their records, and receive an accounting of disclosures.

# HIPAA (Health Insurance Portability and Accountability Act)

Security Rule: Mandates safeguards to protect the electronic storage and transmission of PHI. This includes implementing access controls, data encryption, and audit trails.

Breach Notification Rule: Requires covered entities to notify patients and authorities in case of a breach compromising PHI.

Overall, HIPAA plays a vital role in safeguarding patient privacy and trust in the healthcare system.

# HIPAA (Health Insurance Portability and Accountability Act)

**Start**

Is PHI involved? (Protected Health Information)

Yes --> Enter HIPAA Jurisdiction
No --> Exit (HIPAA not applicable)

HIPAA Jurisdiction

| Rule | Description | Impact on Healthcare |
|---|---|---|
| Privacy Rule | Defines use, disclosure, and access of PHI | Patient access & amendment rights - Standardized authorization forms |
| Security Rule | Requires safeguards for electronic PHI | Data encryption & access controls Regular security assessments |
| Breach Notification Rule | Mandates reporting data breaches | Patient & HHS notification requirements - Time-sensitive reporting deadlines |

**Compliance**
- Implement required safeguards & procedures
- Train staff on HIPAA regulations
- Conduct regular risk assessments

**Non-Compliance**
- Potential civil and criminal penalties
- Financial fines
- Reputational damage

**End**

# Security Measures for Health Information

- Safeguarding Health Information: A 3-Pronged Approach

Protecting patient privacy requires a multi-layered approach. Here's a breakdown of three key safeguards for health information:

❖ Technical Safeguards (ePHI):

- Focuses on securing electronic health records (EHRs).
- Examples include:
  - ✓ Encryption: Scrambling data to make it unreadable without a decryption key.
  - ✓ Access Controls: Limiting access to EHRs only to authorized personnel.
  - ✓ Audit Trails: Tracking user activity and data changes for accountability.

# Security Measures for Health Information

- Physical Safeguards (Paper Records):
  - Protects paper-based health information.
  - Examples include:
    - ✓ Secure Facilities: Limiting physical access to storage areas with security measures like locks and alarms.
    - ✓ Workstation Security: Securing workstations with password protection and user authentication.
    - ✓ Proper Disposal: Following procedures for shredding or destroying paper records with PHI.

# Security Measures for Health Information

❖ Administrative Safeguards (Overall Strategy):

- Establishes a comprehensive security framework for all health information.
- Examples include:
  - ✓ Risk Assessments: Regularly identifying potential threats and vulnerabilities to PHI.
  - ✓ Workforce Training: Educating staff on HIPAA regulations and proper handling of PHI.
  - ✓ Incident Response Plan: Having a plan in place to respond to data breaches or security incidents.

# Security Measures for Health Information flowchart

**Start**

**Is the information in Electronic Health Record (EHR)?**

•Yes --> Implement Technical Safeguards

•No --> Implement Physical Safeguards

**Technical Safeguards (EHR)**

- •Encryption
- •Access Controls
- •Audit Trails

**Physical Safeguards (Paper Records)**

- •Secure Facilities
- •Workstation Security
- •Proper Disposal

**Administrative Safeguards (All Information)**

- •Risk Assessments
- •Workforce Training
- •Incident Response Plan

**End**

# Data Breach Prevention and Response

## Common Causes of Breaches:

- Cyberattacks: Hacking attempts, phishing scams, and malware infections targeting healthcare systems.
- Human Error: Accidental data loss (e.g., lost laptops), unauthorized access by staff, or sending PHI to incorrect recipients.
- Physical Security Issues: Unsecured paper records, unauthorized access to storage facilities, and theft of devices containing PHI.
- Insider Threats: Malicious or careless actions by employees or authorized users.

# Data Breach Prevention and Response

## Recognizing Potential Breaches:

- Unusual activity: Unexplained access attempts, suspicious changes to patient records, or missing devices containing PHI.
- Alerts from security systems: Notifications of potential intrusions, unauthorized data access, or malware infections.
- Patient complaints: Patients reporting receiving incorrect medical information or being contacted by unauthorized individuals.

# Data Breach Prevention and Response

## Responding to a Potential Breach:

- Immediate action: Secure the affected systems, isolate the breach, and contain further data loss.
- Investigate the incident: Identify the cause, determine the scope of the breach, and assess the impact on patients.
- Notify authorities: Report the breach to relevant authorities, such as HIPAA compliance office, depending on the severity.
- Communicate with patients: Inform affected patients about the breach, the information compromised, and steps being taken to address it.

# Data Breach Prevention and Response

## Mitigation Strategies:

- Implement strong technical safeguards: Encryption, access controls, firewalls, and intrusion detection systems.
- Regular security assessments: Identify vulnerabilities and implement corrective measures.
- Employee training: Train staff on HIPAA regulations, data security best practices, and recognizing phishing attempts.
- Physical security measures: Secure facilities, workstations, and proper disposal procedures for paper records.
- Incident response plan: Establish a clear plan for identifying, investigating, and responding to data breaches.

# Data Breach Prevention and Response

By understanding these causes, recognizing potential breaches, and implementing proactive mitigation strategies, healthcare professionals can significantly reduce the risk of data breaches and protect patient privacy.

# Patient Consent and Authorization

- Explore informed consent and its role in sharing health information.
- Discuss situations where patient authorization is required for disclosure.
- Highlight exceptions to consent (e.g., emergencies, public health).

# Interoperability and Health Information Exchange

- Explain the importance of interoperability for seamless data exchange.
- Discuss standards (e.g., HL7, FHIR) and protocols used in health information exchange.
- Address challenges related to data sharing across different systems.

# Emerging Technologies and Privacy Challenges

- Explore the impact of artificial intelligence (AI) and machine learning on health data privacy.
- Discuss the ethical considerations when using AI algorithms for diagnosis and treatment.
- Encourage critical thinking about balancing innovation with patient privacy.

# Case Studies and Practical Scenarios

- Present real-world examples of privacy breaches and security incidents.
- Engage students in analyzing these cases and proposing preventive measures.
- Foster a proactive mindset toward safeguarding health information.

# Case Studies and Practical Scenarios

- Present real-world examples of privacy breaches and security incidents.
- Engage students in analyzing these cases and proposing preventive measures.
- Foster a proactive mindset toward safeguarding health information.


THANK YOU!