

Introduction to Healthcare Information Security

Introduction to Healthcare Information Security

Purpose: Provide a concise, easy-to-read overview for students, new staff, or anyone beginning to work with healthcare data.

1. Why Security Matters in Healthcare

Reason	Explanation
Patient Safety	Incorrect or tampered data can lead to wrong diagnoses, medication errors, or unsafe procedures.
Legal & Regulatory Compliance	Laws such as HIPAA (U.S.), GDPR (EU), PIPEDA (Canada), and local health information acts impose strict privacy and security obligations.
Financial Impact	Breaches cost organizations millions in fines, remediation, and loss of reputation.
Trust & Reputation	Patients expect confidentiality; loss of trust reduces engagement and can damage the institution's brand.
Operational Continuity	Ransomware or system failures can halt clinical workflows, delaying care.

2. Core Concepts & Terminology

Term	Definition
PHI (Protected Health Information)	Any individually identifiable health information, whether electronic, paper, or oral.
Confidentiality, Integrity, Availability (CIA Triad)	The three pillars of information security: keep data private, accurate, and accessible when needed.
Risk Assessment	Systematic process to identify threats, vulnerabilities, and potential impact on PHI.
Threat	Any circumstance or event that could cause loss of CIA (e.g., malware, insider misuse).
Vulnerability	Weakness in a system, process, or control that can be exploited (e.g., unpatched software).

Introduction to Healthcare Information

Term

Definition

Security

Encryption

Transferring data into a coded format that can only be read with the correct key.

Access Control

Policies and mechanisms (e.g., role-based access) that limit who can view or modify data.

Audit Trail

Record of who accessed/changed data, when, and what was done—essential for accountability.

Incident Response

Pre-planned actions taken when a security event occurs (contain, eradicate, recover, post-mortem).

3. Regulatory Landscape (U.S. focus, with global references)

Regulation	Scope	Key Requirements
HIPAA (Health Insurance Portability and Accountability Act)	All “covered entities” (providers, plans, clearinghouses) & business associates.	• Privacy Rule (PHI use/disclosure) • Security Rule (technical, physical, administrative safeguards) • Breach Notification Rule
HITECH Act	Extends HIPAA, encourages adoption of electronic health records (EHR).	• Mandatory breach reporting • Increased penalties for non-compliance
NIST SP 800-53 & 800-66	Framework for federal information systems, adapted for health.	• Controls catalog (access, audit, incident response) • Guidance for protecting ePHI
GDPR	Applies to any organization processing EU residents’ data.	• Data protection by design & default • Right to be forgotten, breach notification within 72h

Introduction to Healthcare Information Security

Regulation	Scope	Key Requirements
State-level laws (e.g., CCPA, NY SHIELD)	Vary by jurisdiction, often add notification, data minimization, or encryption mandates.	• Specific breach notification timelines • Additional consumer rights

Tip: Maintain a **regulatory matrix** that maps each law to the controls you have in place.

4. Security Controls for Healthcare Environments

4.1 Administrative Controls

- **