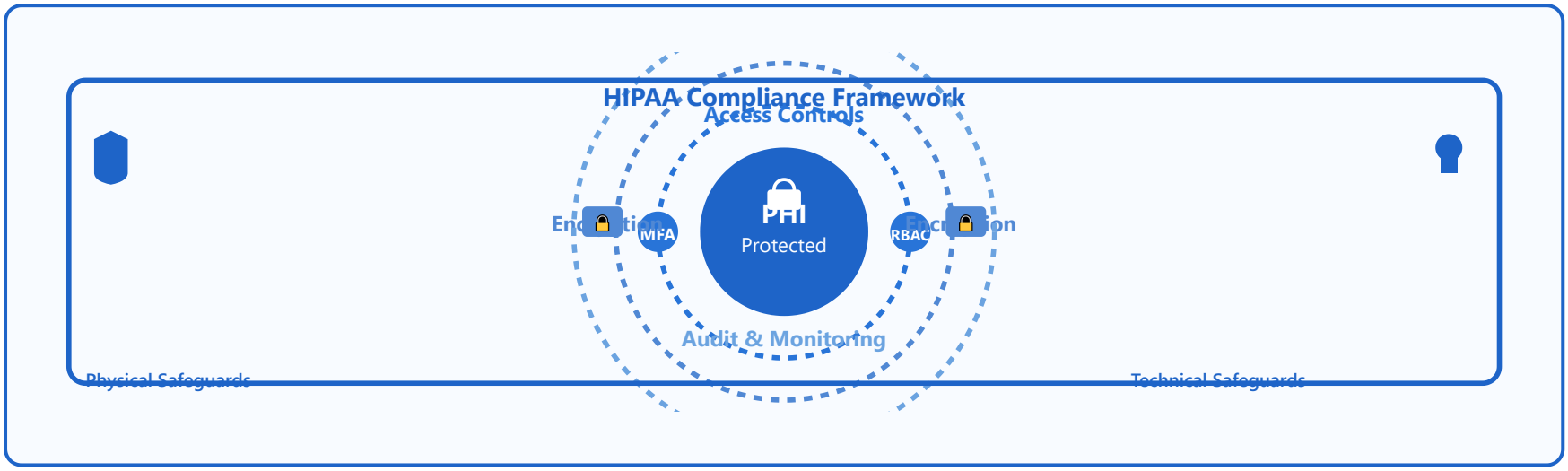
Privacy and HIPAA



PHI Definition

- 18 identifiers under HIPAA
- Names, addresses, dates
- Medical record numbers
- Biometric identifiers

Minimum Necessary Rule

- Access only what's needed
- Role-based permissions
- Need-to-know principle
- Limit data sharing

Access Controls

- User authentication (MFA)

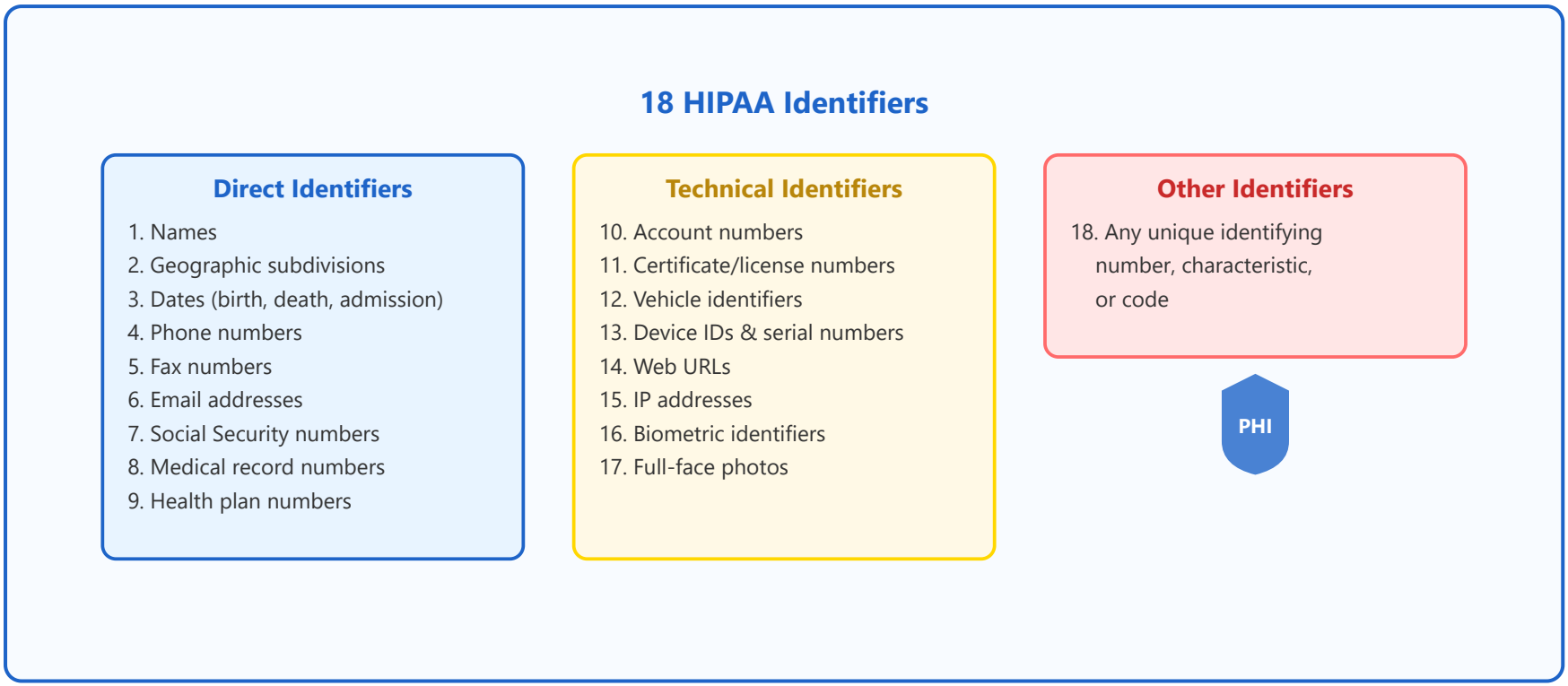
Breach Notification

- Report within 60 days

- Authorization levels
- Audit logs
- Encryption at rest & in transit

- Notify affected individuals
- Inform HHS if >500 patients
- Penalties for non-compliance

1. Protected Health Information (PHI) - Detailed Overview



What is Protected Health Information?

Protected Health Information (PHI) is any information in a medical record that can be used to identify an individual and that was created, used, or disclosed in the course of providing healthcare services. Under HIPAA's Privacy Rule, PHI includes 18 specific identifiers that must be protected to ensure patient privacy.

PHI encompasses three main categories: Direct Identifiers (personal information like names and contact details), Technical Identifiers (digital and system-related identifiers), and Biometric/Visual Identifiers (unique physical characteristics and images).

Real-World Example

Scenario: A hospital database contains patient records with names, dates of birth, medical record numbers, diagnosis codes, and treatment histories.

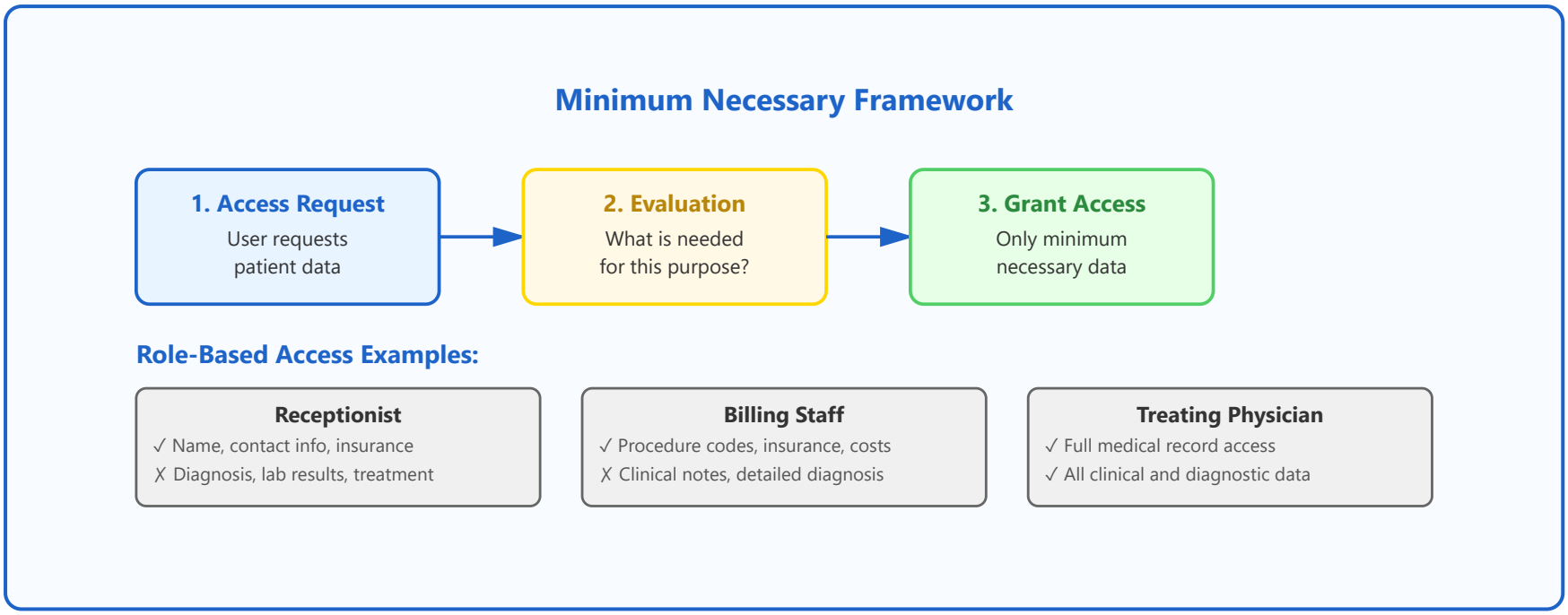
PHI Elements: The patient's name (identifier #1), date of birth (identifier #3), and medical record number (identifier #8) are all PHI. Even the diagnosis and treatment information becomes PHI when linked to these identifiers.

De-identification: If all 18 identifiers are removed, the data becomes de-identified and is no longer subject to HIPAA restrictions.

Key Compliance Points

- ✓ All 18 identifiers must be removed for data to be considered de-identified
- ✓ PHI includes both paper and electronic records
- ✓ Even small geographic areas (less than 20,000 people) are considered identifiers
- ✓ Photographs and comparable images of the full face are PHI
- ✓ Ages over 89 must be aggregated to protect patient privacy

⚖️ 2. Minimum Necessary Rule - Detailed Overview



Understanding the Minimum Necessary Standard

The Minimum Necessary Rule requires covered entities to make reasonable efforts to limit the use, disclosure, and requests for PHI to the minimum necessary to accomplish the intended purpose. This principle is fundamental to HIPAA compliance and protects patient privacy by preventing unnecessary exposure of sensitive information.

Organizations must implement policies and procedures that limit who has access to PHI and what information they can access based on their role and responsibilities. This is typically accomplished through Role-Based Access Control (RBAC) systems that automatically enforce these restrictions.

📋 Real-World Example

Scenario: A nurse needs to schedule a follow-up appointment for a patient.

Minimum Necessary: The nurse needs access to the patient's name, contact information, and appointment history. They do NOT need access to detailed lab results, psychiatric notes, or financial information.

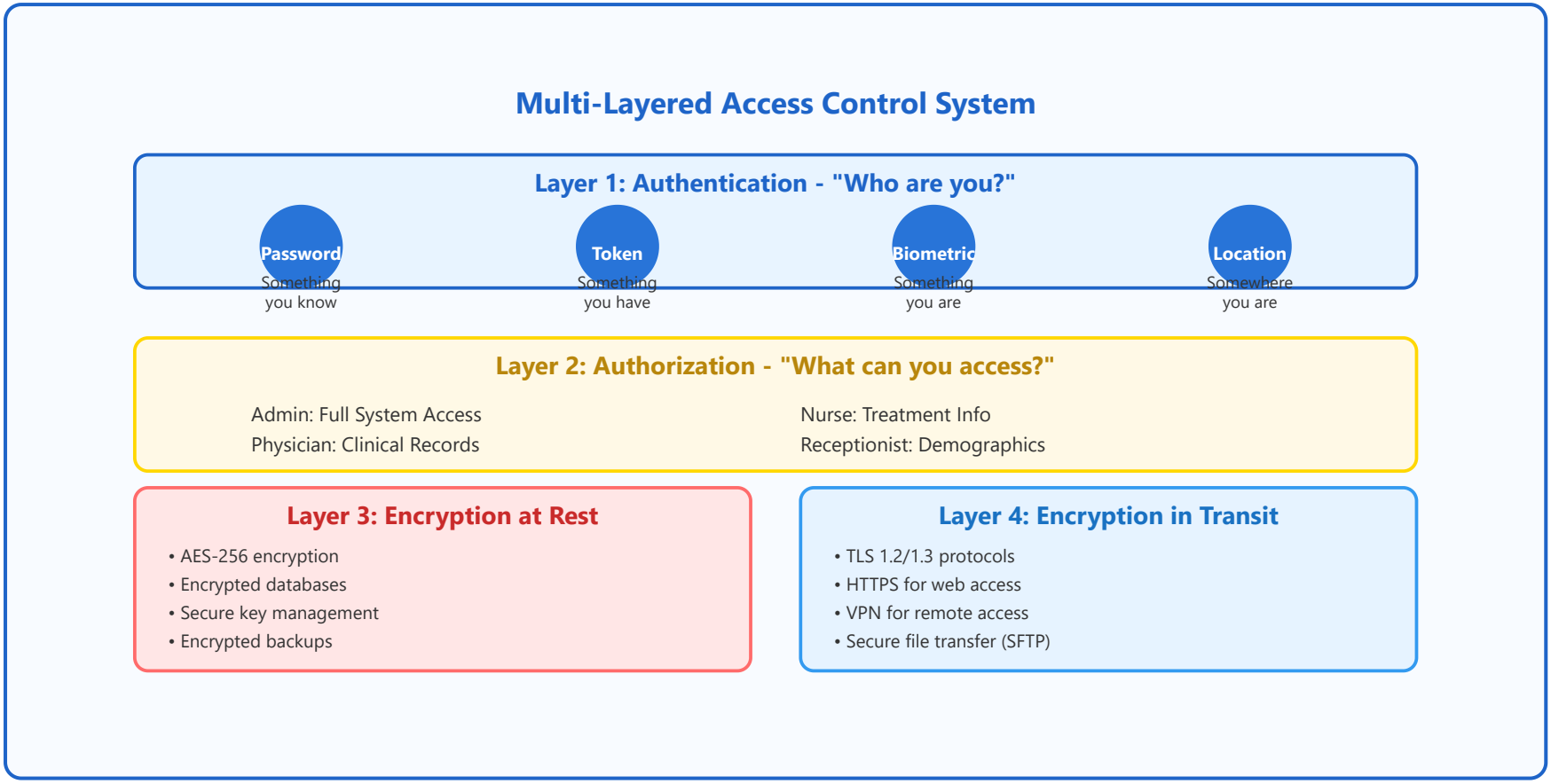
Implementation: The scheduling system should be configured to display only scheduling-relevant information, with clinical details hidden unless specifically needed for that user's role.

Violation Example: Allowing all staff to browse the full electronic health record "just in case" would violate the minimum necessary rule.

Key Compliance Points

- ✓ Document the justification for access levels in organizational policies
- ✓ Regularly review and update role-based access controls
- ✓ Train staff on accessing only what they need for their job functions
- ✓ The rule does NOT apply to treatment purposes or patient-authorized disclosures
- ✓ Implement technical safeguards to enforce minimum necessary automatically

3. Access Controls - Detailed Overview



Comprehensive Access Control Strategy

Access controls are technical safeguards that regulate who can view or use PHI in an electronic information system. HIPAA requires a multi-layered approach combining authentication (verifying identity), authorization (determining permissions), and encryption (protecting data) to create a robust security framework.

Modern healthcare systems implement defense-in-depth strategies where multiple security layers work together. Even if one layer is compromised, other layers continue to protect sensitive patient information. This includes

technical controls (like encryption and firewalls), administrative controls (like policies and training), and physical controls (like locked server rooms).

📋 Real-World Example

Scenario: Dr. Smith needs to access patient records from home during an emergency.

Layer 1 - Authentication: Dr. Smith enters their username and password, then receives a code on their registered mobile device (MFA).

Layer 2 - Authorization: The system verifies Dr. Smith's role and grants access only to records of their assigned patients.

Layer 3 - Encryption at Rest: Patient data stored on the server is encrypted using AES-256.

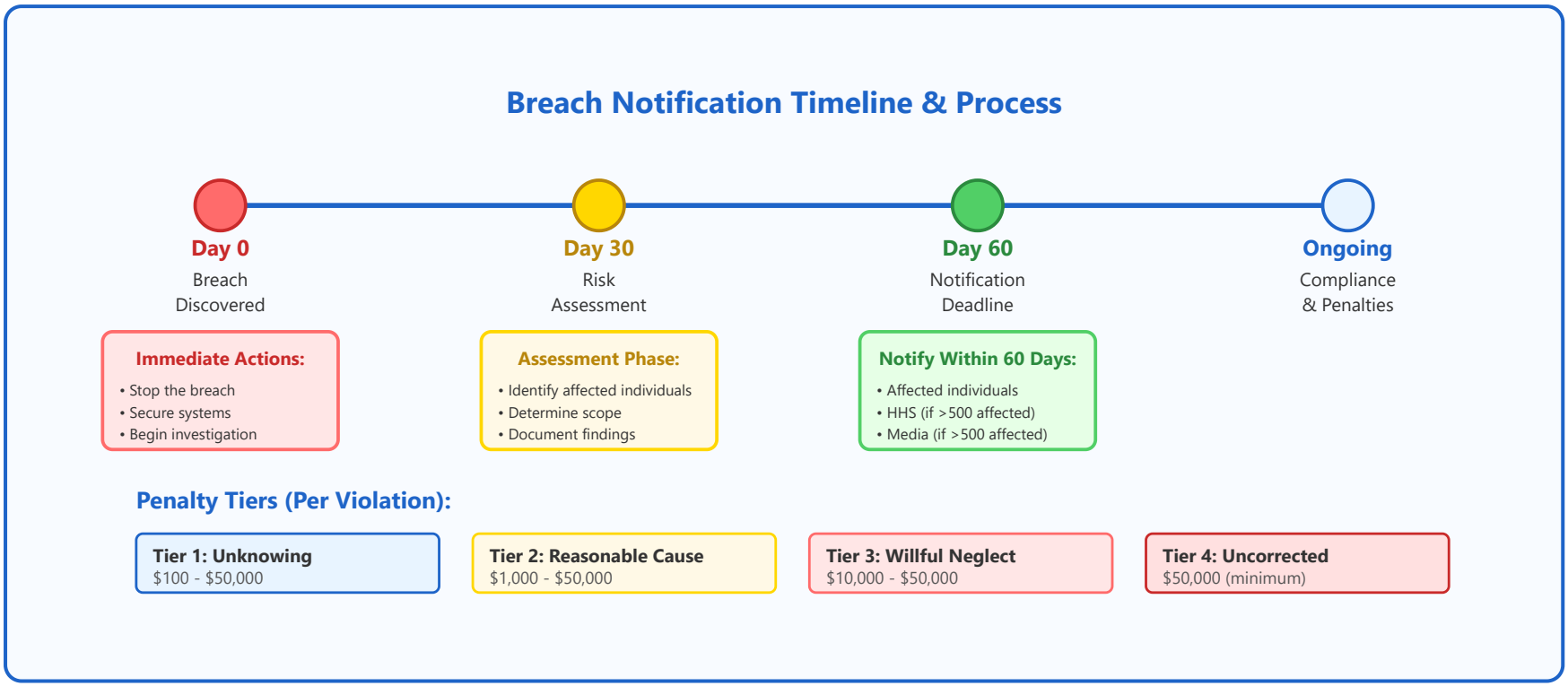
Layer 4 - Encryption in Transit: All data transmitted between Dr. Smith's device and the hospital server is protected by TLS 1.3.

Layer 5 - Audit Trail: The system logs Dr. Smith's access time, IP address, and which records were viewed.

Key Compliance Points

- ✓ Implement multi-factor authentication (MFA) for all system access
- ✓ Use strong encryption (AES-256 for data at rest, TLS 1.2+ for data in transit)
- ✓ Maintain comprehensive audit logs of all PHI access for at least 6 years
- ✓ Implement automatic session timeouts for inactive users
- ✓ Regularly review and update access permissions when roles change
- ✓ Use unique user IDs - never share login credentials

⚠ 4. Breach Notification - Detailed Overview



Understanding HIPAA Breach Notification Requirements

A breach is defined as an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. When a breach occurs, HIPAA's Breach Notification Rule requires covered entities to notify affected individuals, the Department of Health and Human Services (HHS), and in some cases, the media. The notification timeline and requirements depend on the number of individuals affected.

Organizations must conduct a risk assessment to determine if an incident constitutes a reportable breach. This assessment considers factors such as the nature and extent of PHI involved, who accessed the information, whether it was actually acquired or viewed, and the extent to which risk has been mitigated. Not all security incidents are reportable breaches, but thorough documentation is essential.

📋 Real-World Example

Scenario: A hospital laptop containing unencrypted PHI of 800 patients is stolen from an employee's car.

Day 0-5: The theft is discovered. The hospital immediately reports to local police, deactivates the laptop's network access, and begins investigating the scope of compromised data.

Day 5-30: IT conducts a forensic analysis to determine exactly which patient records were on the laptop. Legal and compliance teams assess the risk level.

Day 45: Individual notification letters are sent to all 800 affected patients by first-class mail, including: description of the breach, types of information involved, steps being taken, what patients can do to protect themselves, and contact information.

Day 55: HHS is notified via their breach reporting portal. Since >500 individuals are affected, the hospital also issues a press release and notifies major media outlets.

Outcome: HHS investigates and finds the hospital violated the encryption requirements. The hospital faces penalties of $150,000 and must implement a corrective action plan including mandatory encryption and enhanced security training.

Key Compliance Points

- ✓ Notify affected individuals within 60 days of breach discovery
- ✓ Notify HHS within 60 days if >500 individuals affected (immediately for breaches affecting <500)
- ✓ Notification must include: what happened, types of information involved, steps taken, and what individuals should do
- ✓ Media notification required if >500 residents of a state/jurisdiction affected
- ✓ Maintain documentation of all security incidents for 6 years
- ✓ Annual reporting to HHS for breaches affecting <500 individuals
- ✓ Penalties can reach $1.5 million per violation category per year