TOP HIPAA VIOLATIONS IN 2025

ADMINISTRATIVE & GOVERNANCE GAPS

1 Failure to Conduct Comprehensive Risk Assessments

Vulnerability: Unknown security blind spots.

Reality: Outdated or incomplete risk analyses.

2 Delayed Breach Notification

Vulnerability: Missing mandatory reporting timelines.

Reality: Slow detection and response resulting in missed federal notifications.

3 Insufficient Security Incident Response

Vulnerability: Unprepared for cyber incidents.

Reality: Struggle due to no tested response plans to contain attacks and restore operations.

TECHNICAL & ACCESS VULNERABILITIES

4 Inadequate Access Controls

Vulnerability: Too many users have access to sensitive data.

Reality: Shared accounts, excessive privileges, and poor access reviews.

5 Unencrypted Patient Data

Vulnerability: PHI remains readable if devices are lost or stolen.

Reality: A single unencrypted laptop, smartphone, or storage device can trigger a reportable breach.

6 Poor Audit Log Monitoring

Vulnerability: No visibility into suspicious activity.

Reality: Unauthorized access goes undetected when logs aren't reviewed regularly.

HUMAN & THIRD-PARTY RISKS

7 Weak Third-Party Risk Management

Vulnerability: Vendor security is assumed rather than verified.

Reality: Business Associates become the source of healthcare breaches when oversight is inadequate.

8 Unauthorized Access to PHI

Vulnerability: Insider snooping and misuse.

Reality: Employees accessing records without a legitimate business need continue to generate HIPAA violations.

9 Lack of Employee Training

Vulnerability: The human firewall fails.

Reality: Phishing, social engineering, and accidental disclosures stem from insufficient security awareness.

10 Improper Disposal of PHI

Vulnerability: Sensitive data remains recoverable.

Reality: Unshredded paper records and improperly sanitized devices expose confidential information.

HEALTHCARE COMPLIANCE ESSENTIALS

ASSESS
Conduct annual organization-wide risk assessments.

RESTRICT
Enforce least-privilege access across all systems.

ENCRYPT
Protect PHI at rest and in transit.

AUDIT
Continuously monitor access logs and security events.

TRAIN
Deliver frequent security awareness training.

www.ampcuscyber.com | letsconnect@ampcuscyber.com