HIPAA Compliance for IT Leaders

A practical guide to HIPAA technical safeguards for organizations handling protected health information (PHI). Covers access controls, encryption, audit logging, and breach notification.

Technical Safeguard Requirements

HIPAA's Security Rule requires covered entities and business associates to implement technical safeguards that protect ePHI. These are the required (R) and addressable (A) specifications:

Safeguard	Spec	Status	Implementation Notes
Access Control	Unique User ID	R	Every user has a unique identifier — no shared accounts
	Emergency Access	R	Documented procedure for accessing ePHI during emergencies
	Automatic Logoff	A	Sessions timeout after 15 minutes of inactivity
	Encryption at Rest	A	AES-256 for databases, file systems, backups containing ePHI
Audit Controls	Audit Logging	R	Log all access to systems containing ePHI (who, what, when)
	Log Review	R	Regular review of audit logs for unauthorized access
Integrity	Data Integrity	A	Checksums or digital signatures to verify ePHI not altered
	Transmission Security	R	TLS 1.2+ for all ePHI in transit; VPN for remote access
Authentication	Entity Auth	R	MFA for all users accessing ePHI systems

Breach Notification Requirements

- Individual notification within 60 days of discovery
- HHS notification within 60 days (if 500+ individuals affected, immediate)
- Media notification required if 500+ individuals in a single state
- Business associates must notify covered entity within agreed timeframe
- Document all breach assessments — even those determined to be non-reportable

Common Audit Findings

- Lack of complete, accurate asset inventory of systems containing ePHI
- Missing or incomplete risk assessment (required annually)
- No documented policies and procedures (or outdated versions)
- Shared user accounts or lack of MFA on ePHI systems
- Insufficient audit logging or no regular log review process
- Backup/DR plan not tested (must test at least annually)
- Business Associate Agreements missing or not current

Quick-Start Action Items

- Conduct a risk assessment (required, and the foundation for everything else)
- Enable MFA on all systems that access ePHI

- Encrypt ePHI at rest (database TDE, disk encryption) and in transit (TLS 1.2+)
- Implement audit logging and schedule monthly log reviews
- Review and update BAAs with all vendors who touch ePHI
- Train all workforce members annually on HIPAA awareness
- Test your backup/DR plan — don't just assume it works

Need expert help? Contact AnswerPoint for a free consultation.

216-340-9181 | glenn.mcgregor@answerpoint.com | answerpoint.com/assessment