5-Step HIPAA Readiness Checklist (2025)

STEP 1

Refresh Your Risk Analysis

□ Inventory all systems, applications, and devices that store or process ePHI.
□ Assign risk ratings (likelihood × impact) to identified threats.
□ Document mitigation strategies for high-risk items.
□ Schedule regular updates—annually or when major changes occur.
□ Use the HHS Security Risk Assessment Tool as a guide.

STEP 2

Lock Down Remote Access and Admin Accounts

□ Implement multi-factor authentication (MFA) for all remote access.
□ Apply MFA for accounts with elevated privileges.
□ Remove shared admin credentials and enforce unique logins.
□ Limit remote access to only what is necessary.
□ Log and monitor all access attempts.

STEP 3

Encrypt Data at Rest and in Transit

□ Implement multi-factor authentication (MFA) for all remote access.
□ Apply MFA for accounts with elevated privileges.
□ Remove shared admin credentials and enforce unique logins.
□ Limit remote access to only what is necessary.
□ Log and monitor all access attempts.

Actionable tip: If you're using laptops, mobile devices, or external drives that store ePHI, enable full-disk encryption with solutions like BitLocker (Windows) or FileVault (Mac). For server-side encryption in your EHR or cloud backups, confirm that both data at rest and data in transit are covered—check for TLS 1.2+ and AES-256 standards.

STEP 4

Test Your Incident Response Plan

□ Create or review your written incident response plan.
□ Include contact info for legal counsel, cyber insurance, and IT partners.
□ Ensure you can restore critical systems within 72 hours.
□ Conduct at least one tabletop exercise annually.
□ Log lessons learned from simulations and update the plan accordingly.

Actionable tip: Simulate scenarios that reflect your environment: a phishing attack that compromises login credentials, a ransomware strike on your EHR, or a vendor breach that exposes patient data. During the drill, confirm that everyone knows:

- Who leads response efforts
- Where incident checklists are stored
- How to isolate infected systems
- When to notify patients or regulators

STEP 5

Know Where HIPAA Ends and Other Laws Begin

□ Identify and document all personal data, including non-PHI (employee, marketing, etc.).
□ Map where data is stored and shared.
□ Check if you meet thresholds for CPRA, CPA, or other state laws.
□ Implement procedures to respond to consumer data requests.
□ Update privacy policies and breach notification procedures.

Actionable tip: Map your data flows beyond PHI. Where do website forms go? Do you store applicant resumes or employee tax records? Use this map to:

- Identify what data is regulated by state laws like CPRA or CPA
- Update your privacy policy to reflect what you collect
- Implement access controls or encryption on non-HIPAA systems, too

decypher™
TECHNOLOGIES