LI Tech Solutions

LI Tech Solutions — HIPAA Readiness Checklist

LI Tech Solutions

LI Tech Solutions — HIPAA Readiness Checklist

Use this checklist to quickly assess your practice's current compliance posture—and understand where gaps might exist.

This guide is designed for busy healthcare professionals who may not have a full-time compliance officer or IT department. It breaks HIPAA requirements into everyday, understandable actions. If you're unsure about a term or item, that's a signal it may be time to take a closer look.

As you go through the list, you'll get a clearer picture of your exposure—and where expert support might make the difference. If gaps show up, that's where LI Tech can help.

Instructions:

For each item, check the box **only if the statement is true and currently implemented** in your practice.

Items marked [CRITICAL] are core to HIPAA enforcement and may carry higher regulatory risk if left unaddressed.

LI Tech Solutions

1. Risk Assessment & Review

We have completed a HIPAA risk assessment within the last 12 months. This means your practice has formally reviewed potential risks to ePHI since last year and has documentation to prove it.

[CRITICAL]

[ ] **Our risk assessment includes physical, technical, and administrative safeguards.** This means your analysis reviewed physical access, IT system protections, and organizational policies that impact patient data.

[ ] **We review and update our risk posture after any major system or vendor change.** You've re-evaluated HIPAA risks following events like a new EHR, office relocation, or onboarding a cloud provider.

2. Access Control & Credentialing

[CRITICAL]

[ ] **Each staff member has a unique login (no shared credentials).** Every user who accesses PHI uses an individual ID that can be traced to their activity.

[ ] **We use strong passwords and two-factor authentication where possible.** Passwords are complex and 2FA is implemented for systems that manage patient data.

[ ] **Access is restricted based on job role.** Staff members only have access to the data necessary for their specific responsibilities.

3. Device & Data Security

[CRITICAL]

[ ] **All devices handling ePHI are encrypted.** Laptops, phones, tablets, and desktops that access PHI use encryption to protect stored and transmitted data.

[ ] **We use secure, private Wi-Fi.** All network traffic involving PHI occurs over password-protected and encrypted wireless networks.

[ ] **Lost or stolen devices can be remotely wiped.** You have a documented process and tool in place to erase sensitive data if a device goes missing.

4. Backups & Recovery

[CRITICAL]

[ ] **We have regular, automated backups of systems that handle ePHI.** Data is backed up at least weekly and without manual steps.

[ ] **Backups are encrypted and stored securely.** Backup copies are encrypted and stored in secure locations or cloud services that meet HIPAA requirements.

[ ] **We have tested our ability to restore from backup in the last 6 months.** You've recently performed a test restoration of critical data and confirmed success.

5. Policies & Documentation

[ ] **We maintain written policies for HIPAA-related procedures.** These cover things like access control, device use, breach response, and employee conduct.

[ ] **We document and review those policies annually.** There is a record of policy review at least once per calendar year.

[CRITICAL]

[ ] **We maintain signed Business Associate Agreements (BAAs) with all vendors handling PHI.** These include billing platforms, EHRs, and any third parties with access to patient data.

6. Staff Training & Awareness

[CRITICAL]

[ ] **All staff receive annual HIPAA compliance training.** This includes new hires and part-time workers, with documentation of attendance.

[ ] **Staff know how to identify and report a potential breach.** Employees understand what constitutes a breach and who to notify.

[ ] **We conduct occasional audits or spot checks.** Your organization performs informal checks on access logs, policy adherence, or physical security.

7. Incident Response & Monitoring

[CRITICAL]

[ ] We have a written breach response plan. A document exists detailing roles, timelines, and regulatory steps if a breach occurs.

[ ] We maintain audit logs and monitor access to ePHI. Logs are retained and reviewed periodically to detect unauthorized access.

[ ] We know our process for reporting a HIPAA incident or breach. Your team knows how to notify HHS and affected parties, including timeframes and documentation required.

How to Interpret Your Results

This checklist is not a legal compliance test—but it helps highlight where your practice may benefit from expert support:

0–5 Unchecked: You're likely covering most of your bases. A consult can help you validate and document your safeguards.

6–10 Unchecked: You've got some gaps that deserve attention. Closing them now can help avoid future risk.

11+ Unchecked: High exposure. A structured HIPAA review should be scheduled as soon as possible.

Even one gap—if it's critical (like lack of a breach plan or missing BAAs)—can trigger enforcement issues. Let's talk.High risk. Immediate review strongly recommended.

How to Interpret Your Results

LI Tech Solutions helps Long Island medical practices close gaps, document safeguards, and stay audit-ready.
Schedule a HIPAA Readiness Consult →