

HEALTHCARE AND MEDICAL

HIPAA IT Compliance Checklist

The technical safeguards an auditor, an insurer, and a ransomware crew will all check first.

HIPAA does not tell you which firewall to buy. It tells you to know where patient data lives, control who can reach it, and prove it. Most Boston-area practices we meet are closer than they think, and the gaps are almost always the same handful of items below.

How to use it: tick what you have in place today. Anything left unticked is a conversation worth having.

01 Know where ePHI lives

- ☐ **Written security risk analysis, updated this year**
The Security Rule requires it. It is also the first document OCR asks for after a breach.
- ☐ **Inventory of every system that stores or touches patient data**
EHR, imaging, billing, fax, email, scanners, and the laptop the office manager takes home.
- ☐ **Business associate agreements on file for every vendor with access**
EHR vendor, billing company, IT provider, cloud backup, shredding service.
- ☐ **Patient data kept off personal phones and personal email**
Use managed apps with the ability to wipe practice data remotely.
- ☐ **Retired devices wiped or destroyed with a certificate**
Copiers and old workstations keep data on internal drives.

02 Control and protect access

- ☐ **Unique logins for every staff member, no shared accounts**
Shared front-desk passwords make audit logs worthless.
- ☐ **Multi-factor authentication on email, EHR, and remote access**
The single control insurers ask about most.
- ☐ **Automatic screen lock and session timeouts on clinical workstations**
Five to ten minutes in patient areas.
- ☐ **Encryption on every laptop, phone, and backup**
An encrypted lost laptop is usually not a reportable breach. An unencrypted one is.
- ☐ **Endpoint detection and response on every device, monitored 24/7**
Antivirus alone does not stop modern ransomware.
- ☐ **Offboarding checklist that removes access the same day**
Former staff with live EHR or email access is a common audit finding.

03 Prove it and recover

- ☐ **Audit logging turned on and reviewed**
Who opened which chart, when, and from where.
- ☐ **Daily backups, one copy offline or immutable, restore tested quarterly**
Untested backups fail at the worst moment.
- ☐ **Written incident response plan with breach notification steps**
HIPAA and Massachusetts law (Chapter 93H) both set notification duties.
- ☐ **Annual security awareness training plus phishing simulations**
Keep the completion records. They count as evidence.
- ☐ **Outage plan: cloud or off-site copies outside the building**
Nor'easters and power cuts happen. Plan for a day without the office.

Red flags we see most

- Your risk analysis is more than a year old, or you have never seen one.
- The EHR login is written on a sticky note.
- Backups go to a USB drive that stays in the office.
- Nobody can tell you who still has remote access.

Where to start

Start with the risk analysis. It turns this checklist into a ranked to-do list and it is the document that protects you most if something goes wrong.

Want a second set of eyes?

Book a free 30-minute technical assessment. A senior engineer walks through this checklist with you and tells you what to fix first. No sales script, no obligation.

Book a technical assessment

(617) 322-5155

bostonmit.com/it-assessment