DOWNLOADABLE WORKSHEET · CYBERSECURITY

HIPAA IT Requirements *Self-Audit* Checklist

A working document for IT directors, practice administrators, and compliance officers at healthcare organizations. Built around one premise: everything an investigator would ask you is something you can ask yourself first — while the answers are still cheap to fix.

How to use this checklist

Work through the nine sections below with the people who actually run each area — IT, compliance, practice management. Each item is scored on the same three-point scale. Be honest: the goal is to assemble the same picture an auditor would, months or years before anyone asks for it.

Scoring scale

Score	Meaning
0 — Absent	Control does not exist, or no one can answer the question.
1 — Partial	Control exists but is undocumented, untested, out of date, or unevidenced.
2 — Proven	Control is in place AND you can produce the artifact — a document, a log, a report, a signed agreement.

> The "proven" bar is deliberately high: A confident verbal "yes" is a 1, not a 2. An investigator never accepts "we do that" without evidence, so neither should this checklist. If you can't put your hands on the artifact within one business day, score it a 1.

40 items × 2 points = 80 points maximum. Tally at the end and use the scorecard to decide your next step.

S1 — Risk Analysis & Documentation

The first thing an investigator asks for. Is yours current, or a template filled out years ago?

- [ ] 1. Does a written risk analysis exist that identifies where ePHI is created, stored, transmitted, and received? (0 / 1 / 2)
- [ ] 2. Has it been reviewed or updated in the last 12 months — and after every material change (new system, new vendor, remote work, AI tools)? (0 / 1 / 2)
- [ ] 3. Does it cover your actual current environment — cloud services, remote access, mobile devices, and AI tools — not just the on-premises systems of years past? (0 / 1 / 2)

- [ ] 4. Is there a risk management plan showing identified risks were remediated, mitigated, or formally accepted — with dates and owners? (0 / 1 / 2)
- [ ] 5. Are HIPAA policies and procedures documented, versioned, and accessible to the workforce (not a binder no one has opened)? (0 / 1 / 2)

Section S1 subtotal _____ / 10

S2 — Identity & Access Controls

Who can see PHI, why, and who checked?

- [ ] 6. Does every workforce member have a unique login — no shared accounts anywhere PHI is accessible? (0 / 1 / 2)
- [ ] 7. Is access role-based, granting the minimum necessary for each job function? (0 / 1 / 2)
- [ ] 8. Is multi-factor authentication enforced on every system and remote path that touches PHI? (0 / 1 / 2)
- [ ] 9. Are departures deprovisioned within one business day, with a documented offboarding step that proves it? (0 / 1 / 2)
- [ ] 10. Is there a periodic access review (at least annually) that catches stale accounts and permission creep — with records of the last one? (0 / 1 / 2)
- [ ] 11. Do privileged/admin accounts get extra controls — separate credentials, tighter monitoring, a documented list of who holds them? (0 / 1 / 2)

Section S2 subtotal _____ / 12

S3 — Endpoints & Devices

Every device that can reach PHI, accounted for.

- [ ] 12. Is there a complete, current inventory of every laptop, workstation, and mobile device that can access PHI? (0 / 1 / 2)
- [ ] 13. Is full-disk encryption enforced and verifiable per device — could you produce encryption evidence for a specific laptop lost tonight? (0 / 1 / 2)
- [ ] 14. Are devices centrally managed — patched on a defined cadence, screen-lock enforced, remote wipe available? (0 / 1 / 2)
- [ ] 15. Are personal/BYOD devices either blocked from PHI or brought under the same enforced controls? (0 / 1 / 2)
- [ ] 16. Is retired hardware and media sanitized or destroyed with a documented record for each asset? (0 / 1 / 2)

Section S3 subtotal _____ / 10

S4 — Encryption & Data Protection

"Addressable" is not "optional." Can you evidence it?

- [ ] 17. Is ePHI encrypted at rest across servers, databases, backups, and cloud storage? (0 / 1 / 2)

- [ ] 18. Is ePHI encrypted in transit — including email paths, file transfers, and remote access? (0 / 1 / 2)
- [ ] 19. Where encryption was deemed not reasonable, is there a documented rationale and equivalent alternative control (the rule's actual requirement)? (0 / 1 / 2)
- [ ] 20. Are encryption keys and certificates managed — owned, rotated, and not sitting in a spreadsheet? (0 / 1 / 2)

Section S4 subtotal _____ / 8

S5 — Audit Logging & Monitoring

Could you answer "who accessed this record on this date?"

- [ ] 21. Do audit logs capture PHI access — who, what, when — on every system holding ePHI? (0 / 1 / 2)
- [ ] 22. Are logs retained per a defined policy and protected from tampering or quiet overwrites? (0 / 1 / 2)
- [ ] 23. Does someone actually review logs on a defined cadence — with alerting for anomalies, not just collection? (0 / 1 / 2)
- [ ] 24. Could you reconstruct a specific access event (e.g., a suspected snooping incident) within one business day? (0 / 1 / 2)

Section S5 subtotal _____ / 8

S6 — Backup, Retention & Contingency

The rule requires recovery, not just backup jobs.

- [ ] 25. Are all systems containing ePHI backed up, with at least one copy protected from ransomware (immutable or offline)? (0 / 1 / 2)
- [ ] 26. Has a restore been tested and documented in the last 12 months — an actual recovery, not a green checkmark on a job? (0 / 1 / 2)
- [ ] 27. Is there a written contingency plan (emergency mode + disaster recovery) that keeps critical patient-facing systems available during an outage? (0 / 1 / 2)
- [ ] 28. Do retention and disposal policies exist and match your legal and clinical requirements — with disposal actually happening on schedule? (0 / 1 / 2)

Section S6 subtotal _____ / 8

S7 — Vendor & BAA Inventory

Every third party that touches PHI, under a signed agreement.

- [ ] 29. Is there a living inventory of every vendor that creates, receives, stores, or transmits PHI on your behalf — including the small tools that crept in sideways? (0 / 1 / 2)
- [ ] 30. Could you produce a signed BAA for every vendor on that list within one business day? (0 / 1 / 2)

- [ ] 31. Do you assess vendor security posture — requesting SOC 2 reports or equivalent evidence, not just the signature? (0 / 1 / 2)
- [ ] 32. Is there a process that catches new vendors before PHI flows — so the BAA comes first, not after adoption? (0 / 1 / 2)

Section S7 subtotal _____ / 8

S8 — Workforce Training & Awareness

Real, recurring, documented — and specific to how your people work.

- [ ] 33. Does every workforce member complete HIPAA training at onboarding and at least annually — with completion records you can produce? (0 / 1 / 2)
- [ ] 34. Is training specific to your environment and roles (front desk vs. clinical vs. IT), not a generic annual slideshow? (0 / 1 / 2)
- [ ] 35. Do staff know how to report a suspected incident or violation — and is there evidence reports actually get made and handled? (0 / 1 / 2)

Section S8 subtotal _____ / 6

S9 — AI & Emerging Tools

The section that wasn't in your last risk analysis — and the first place shadow usage hides.

- [ ] 36. Does a written AI usage policy exist — approved tools, prohibited tools, and what data may never be entered into any AI tool? (0 / 1 / 2)
- [ ] 37. Do you know which AI tools staff actually use — from technical discovery (DNS/web filtering, SaaS discovery), not just which ones you approved? (0 / 1 / 2)
- [ ] 38. Is every AI tool that touches PHI under a signed BAA — with consumer/free tiers explicitly blocked or prohibited? (0 / 1 / 2)
- [ ] 39. For ambient/scribe AI in clinical settings: are retention, model-training use, and audit trails documented in writing before go-live? (0 / 1 / 2)
- [ ] 40. Has the workforce been specifically trained on PHI and AI — why pasting patient information into a chatbot is a reportable problem, and what the sanctioned alternative is? (0 / 1 / 2)

Section S9 subtotal _____ / 10

Red-Flag Summary — 8 Findings That End Audits Badly

Any single item here should trigger remediation now — these are the patterns investigators find over and over, and none of them survives an OCR file review.

- [ ] R1. The risk analysis is missing, or is a template last touched years ago.
- [ ] R2. A vendor touching PHI has no signed BAA.

- [ ] R3. A device that can reach PHI has no provable encryption.
- [ ] R4. Audit logs exist but no one has ever reviewed them.
- [ ] R5. Shared logins anywhere PHI is accessible.
- [ ] R6. No restore has ever been tested — backup "works" only as a job status.
- [ ] R7. Staff are using AI tools with PHI and no one can say which tools or what data.
- [ ] R8. Departed employees still hold active accounts.

Red flags counted (any > 0 = remediate before anything else on this list) _____ / 8

Scorecard Tally & Next Step

Section	Score	Max
S1 — Risk Analysis & Documentation		10
S2 — Identity & Access Controls		12
S3 — Endpoints & Devices		10
S4 — Encryption & Data Protection		8
S5 — Audit Logging & Monitoring		8
S6 — Backup, Retention & Contingency		8
S7 — Vendor & BAA Inventory		8
S8 — Workforce Training & Awareness		6
S9 — AI & Emerging Tools		10
TOTAL		80

Interpreting your score

Total	What it means	Next step
68–80	A program you could evidence under scrutiny.	Close out the 1s, clear any red flags, put the review on an annual calendar.
50–67	Real gaps — most often in risk analysis currency, BAAs, or logging review.	Remediate the two weakest sections this quarter; re-score in 90 days.
30–49	You have tools, not a provable program — the compliant-stack pattern.	Treat as high-risk; start with the risk analysis and BAA inventory, in that order.
Below 30	An investigation today would become an audit of everything.	Stop and rebuild deliberately — risk analysis first, then access, encryption, and vendors.

> Any red flag overrides the score: A program can total 70 and still be one lost laptop away from a reportable breach if R3 is unresolved.

Next step: bring your two lowest-scoring sections — and every counted red flag — into a working session with your IT and compliance leads. The goal isn't a better number on paper; it's being able to hand over the artifacts, calmly, the day someone asks for them.