HIPAA Risk Analysis Checklist

2026 Edition

RESCOR LLC • www.rescor.net • +1 863 SECURE1 (+1 863 732-8731)

Use this checklist to evaluate your organization's HIPAA Security Rule compliance posture. Each item maps to a specific 45 CFR 164 implementation specification. Items marked (R) are Required; items marked (A) are Addressable.

Administrative Safeguards (45 CFR 164.308)

Risk Analysis & Management

- ☐ Have you performed a risk analysis within the past 12 months? (R) 164.308(a)(1)(ii)(A)
- ☐ Does your risk analysis identify specific threats to specific ePHI assets with quantified risk values?
- ☐ Do you have a documented risk management plan? (R) 164.308(a)(1)(ii)(B)
- ☐ Can you compare this year's risk assessment to last year's and show measurable change?
- ☐ Have you documented your risk tolerance at the Board or executive level?

Governance & Oversight

- ☐ Is there a designated Security Official? (R) 164.308(a)(2)
- ☐ Does an IT steering committee or governance body meet regularly?
- ☐ Are security decisions made with stakeholder input from clinical, admin, financial, and IT?
- ☐ Does executive leadership receive at least annual reporting on the security program?

Workforce Security

- ☐ Procedures for authorizing and supervising workforce access to ePHI? (A) 164.308(a)(3)(ii)(A)
- ☐ Clearance procedures for granting ePHI access? (A) 164.308(a)(3)(ii)(B)
- ☐ Termination procedures include timely revocation of all access — including mobile? (A) 164.308(a)(3)(ii)(C)
- ☐ Verified that terminated employees do not retain access to any systems?

Access Management

- ☐ Policies for granting access based on role and minimum necessary? (R) 164.308(a)(4)(i)
- ☐ Access authorizations documented and reviewed periodically? (A) 164.308(a)(4)(ii)(B)
- ☐ Can you demonstrate who has access to what ePHI and why?

Security Awareness & Training

- ☐ All workforce members receive HIPAA security training at hire and annually? (A) 164.308(a)(5)(ii)(A)

- [ ] Training addresses current threats including phishing, social engineering, and AI risks?
- [ ] Security reminders provided to workforce? (A) 164.308(a)(5)(ii)(A)
- [ ] Procedures for detecting malicious software? (A) 164.308(a)(5)(ii)(B)
- [ ] Log-in attempts monitored? (A) 164.308(a)(5)(ii)(C)

Incident Response

- [ ] Documented security incident response procedures? (R) 164.308(a)(6)(i)
- [ ] Incident response plan is cross-functional — not just IT? 164.308(a)(6)(ii)
- [ ] Plan has been tested (tabletop exercise or drill)?
- [ ] Escalation procedures defined?
- [ ] Plan addresses proposed 72-hour reporting requirement?
- [ ] Forensic investigation capability — internal or contracted?

Contingency Planning

- [ ] Data backup plan? (R) 164.308(a)(7)(ii)(A)
- [ ] Disaster recovery plan? (R) 164.308(a)(7)(ii)(B)
- [ ] Emergency mode operation plan? (R) 164.308(a)(7)(ii)(C)
- [ ] Contingency plans tested and revised periodically? (A) 164.308(a)(7)(ii)(D)
- [ ] Applications and data criticality analysis? (A) 164.308(a)(7)(ii)(E)
- [ ] BCP/DRP addresses EMR platform dependencies?

Evaluation & Business Associates

- [ ] Periodic technical and nontechnical evaluations? (R) 164.308(a)(8)
- [ ] All business associates have current BAAs? (R) 164.308(b)(1)
- [ ] BAAs address AI services that process ePHI?

Physical Safeguards (45 CFR 164.310)

- [ ] Facility security plan? (A) 164.310(a)(2)(ii)
- [ ] Access control and validation procedures? (A) 164.310(a)(2)(iii)
- [ ] Workstation use policies? (R) 164.310(b)
- [ ] Workstations physically secured? (R) 164.310(c)
- [ ] Media disposal procedures? (R) 164.310(d)(2)(i)
- [ ] Media re-use procedures? (R) 164.310(d)(2)(ii)

- [ ] Hardware/media movement accountability? (A) 164.310(d)(2)(iii)
- [ ] Data backup/storage for device transfers? (A) 164.310(d)(2)(iv)

Technical Safeguards (45 CFR 164.312)

- [ ] Every user has a unique identifier? (R) 164.312(a)(2)(i)
- [ ] Emergency access procedures? (R) 164.312(a)(2)(ii)
- [ ] Automatic logoff? (A) 164.312(a)(2)(iii)
- [ ] Encryption for ePHI at rest? (A) 164.312(a)(2)(iv)
- [ ] MFA for remote access and privileged accounts?
- [ ] Audit logging for ePHI systems? (R) 164.312(b)
- [ ] Audit logs reviewed regularly?
- [ ] ePHI authentication mechanisms? (A) 164.312(c)(2)
- [ ] Person/entity authentication? (R) 164.312(d)
- [ ] Encryption for ePHI in transit? (A) 164.312(e)(2)(ii)

Emerging Risk Areas (2026)

AI Governance

- [ ] Formal AI use policy (PAND or DANP)?
- [ ] BAAs in place for AI services processing ePHI?
- [ ] Workforce trained on acceptable AI use and CPPI handling?
- [ ] Process for authorizing new AI tools before use?
- [ ] AI outputs reviewed by qualified humans before clinical use?

Network & Asset Management

- [ ] Network segments documented (clinical, admin, IoT, legacy)?
- [ ] End-of-life systems isolated on segregated VLANs?
- [ ] Current asset inventory of all devices touching ePHI?

Email, Tracking & Vendor Risk

- [ ] AI-based email protections deployed?
- [ ] Patient-facing websites audited for tracking technologies?
- [ ] Vendor platform dependencies in contingency planning?

☐ Risks from M&A and affiliations tracked?

Score Your Results

Section	Items	Your Score	Coverage
Administrative Safeguards	32	___ / 32	___%
Physical Safeguards	8	___ / 8	___%
Technical Safeguards	10	___ / 10	___%
Emerging Risk Areas	12	___ / 12	___%
Total	**62**	**___ / 62**	**___%**

Below 50%: Significant HIPAA exposure. A formal risk analysis should be immediate priority.

50-75%: Common gaps that increase enforcement and breach risk. A structured program addresses these systematically.

Above 75%: Fundamentals covered. Focus on emerging areas and continuous improvement.

What To Do Next

This checklist identifies gaps — it does not replace a formal HIPAA risk analysis. RESCOR performs quantitative risk analysis using STORM methodology that produces the specific, measurable results OCR expects.

Schedule a free 30-minute HIPAA risk consultation:
https://calendly.com/rescorllc/30min

Contact us: +1 863 SECURE1 (+1 863 732-8731) • www.rescor.net/contact

RESCOR LLC • 521 Lincoln Road, West Enfield, ME 04493 • www.rescor.net