



HIPAA Security Rule Readiness Checklist

A Self-Assessment Tool for Healthcare Organizations

Prepared by Sidechain Security | May 2026

The HIPAA Security Rule is undergoing its most significant overhaul since 2003. The proposed changes eliminate the distinction between 'required' and 'addressable' safeguards, make encryption mandatory, require multi-factor authentication, and impose annual security audits, vulnerability scanning, and penetration testing. Organizations will have 240 days to comply.

This checklist helps you assess where your organization stands today against both the current rule and the proposed changes — so you can identify gaps and prioritize action before the compliance clock starts.

Why This Matters

The proposed HIPAA Security Rule update — published in the Federal Register on January 6, 2025 — represents the most significant change to healthcare security requirements in over two decades. Whether the rule is finalized in its current form or not, OCR is already enforcing aggressively under the existing rule. The organizations that prepare now will be ready either way.

21 OCR enforcement penalties in 2025	\$3M Largest fine for risk analysis failure	\$10.93M Average healthcare breach cost	240 Days to comply once rule is finalized
--	---	---	---

The #1 cited deficiency in OCR investigations: Failure to conduct an adequate, enterprise-wide Security Risk Assessment. More than half of 2025 enforcement actions cited this single issue. Fines ranged from \$25,000 to \$3,000,000. Under the proposed rule, the standard for what constitutes an adequate assessment becomes significantly more prescriptive.

The Biggest Changes Coming

- **'Addressable' Is Eliminated.** All implementation specifications become mandatory. No more documenting an alternative instead of implementing the control.
- **Encryption Becomes Mandatory.** All ePHI must be encrypted at rest and in transit using NIST-approved algorithms. This is the single largest change for most organizations.
- **Multi-Factor Authentication Required.** MFA must be implemented for all ePHI system access.
- **Annual Security Risk Assessment.** Must be tied to a technology asset inventory and network map, with documented remediation for identified risks.
- **Vulnerability Scanning & Penetration Testing.** Biannual vulnerability scans and annual pen tests become mandatory.
- **72-Hour System Restoration.** Critical ePHI systems must be restorable within 72 hours of a security incident.
- **Technology Asset Inventory & Network Map.** Comprehensive, documented, reviewed annually.

How to Use This Checklist

The following pages cover each major control area affected by the proposed changes. For each area, you will find: what the current rule requires, what the proposed rule changes, a self-assessment checklist for your organization, and common gaps we find during assessments. Work through each section with your IT team or security lead. Be honest — this is for your benefit, not for show.

At the end, tally your results using the summary scorecard to identify your highest-priority gaps.

1. Security Risk Assessment

§164.308(a)(1) — Security Management Process | CURRENT: Required | PROPOSED: More prescriptive

Why this matters most: This is the single control area OCR cites most frequently in enforcement actions. An inadequate or outdated risk assessment is the fastest path to a penalty — and under the proposed rule, the bar rises significantly.

Control Area	Current Requirement	Proposed Change	Your Status	Action Needed
Risk Analysis	Conduct accurate, thorough assessment of risks to ePHI (Required)	Must be annual, tied to asset inventory, assign risk levels, document remediation actions taken	☐ Yes ☐ Partial ☐ No	If no current assessment exists, this is priority #1
Risk Management	Implement measures to reduce risk to reasonable level (Required)	Must demonstrate that identified risks drove specific control decisions	☐ Yes ☐ Partial ☐ No	Document remediation for every finding
Asset Inventory	Implied but not explicit	Mandatory technology asset inventory of all ePHI systems, reviewed annually	☐ Yes ☐ Partial ☐ No	Inventory all hardware, software, cloud services touching ePHI
Network Map	Implied but not explicit	Mandatory network map showing ePHI flows, reviewed annually	☐ Yes ☐ Partial ☐ No	Document how ePHI moves through your network

Self-Assessment:

- ☐ We have conducted a Security Risk Assessment within the past 12 months
- ☐ Our assessment covers every system that creates, receives, maintains, or transmits ePHI
- ☐ We maintain a current technology asset inventory
- ☐ We have a documented network map showing ePHI flows
- ☐ Each identified risk has a documented treatment decision (mitigate, accept, transfer)
- ☐ We can produce the assessment document for OCR on request
- ☐ Our risk assessment was updated after our most recent system or environment change

Common Gaps We Find:

• Assessment is more than 12 months old or was never performed • Generic template used without organization-specific analysis • No asset inventory feeding the assessment • Risks identified but no remediation tracked • Assessment not updated after major system changes (new EHR, cloud migration, etc.)

2. Encryption

§164.312(a)(2)(iv) and §164.312(e)(2)(ii) — Access Control / Transmission Security | CURRENT: Addressable | PROPOSED: Required

The biggest single change: Encryption has been 'addressable' for 20 years — meaning organizations could document an alternative. Under the proposed rule, encryption of ePHI at rest and in transit becomes mandatory with no exceptions. This will require significant implementation effort for many organizations.

Control Area	Current Requirement	Proposed Change	Your Status	Action Needed
Encryption at Rest	Addressable. Can document alternative.	Mandatory. All ePHI encrypted at rest using NIST-approved algorithms.	☐ Yes ☐ Partial ☐ No	Full disk encryption on all endpoints; database encryption; encrypted backups
Encryption in Transit	Addressable. Can document alternative.	Mandatory. All ePHI encrypted in transit.	☐ Yes ☐ Partial ☐ No	TLS for email; HTTPS for all web apps; encrypted interfaces; VPN for remote
Key Management	Not explicitly addressed	Implied by mandatory encryption requirements	☐ Yes ☐ Partial ☐ No	Document key storage, rotation, and access procedures

Self-Assessment:

- ☐ Full disk encryption is enabled on ALL workstations and laptops (BitLocker / FileVault)
- ☐ Our EHR database encrypts ePHI at rest
- ☐ Backups containing ePHI are encrypted
- ☐ File servers and NAS devices storing ePHI use encryption
- ☐ Email is transmitted using enforced TLS (not opportunistic)
- ☐ All web applications handling ePHI use HTTPS exclusively
- ☐ HL7/FHIR interfaces between systems use encrypted connections
- ☐ Remote access requires VPN with encryption
- ☐ We have documented key management procedures
- ☐ We are NOT using deprecated encryption algorithms (DES, 3DES, RC4, MD5)

Common Gaps We Find:

• Laptops without full disk encryption (critical if lost/stolen) • Database ePHI stored unencrypted • Email can be sent without TLS enforcement • Backups stored unencrypted • Legacy interfaces between systems running unencrypted • Encryption keys stored alongside encrypted data

3. Access Control & Authentication

§164.312(a) and §164.312(d) — Access Control / Person or Entity Authentication | MFA CURRENT: Not explicit | MFA PROPOSED: Required

Control Area	Current Requirement	Proposed Change	Your Status	Action Needed
Unique User IDs	Required. Every user must have unique identifier.	No change — still required. Shared accounts remain non-compliant.	☐ Yes ☐ Partial ☐ No	Eliminate all shared and generic accounts
MFA	Not explicitly required. Authentication method flexible.	MFA mandatory for all ePHI system access.	☐ Yes ☐ Partial ☐ No	Deploy MFA across EHR, email, VPN, cloud apps
Automatic Logoff	Addressable	Mandatory. Sessions must timeout after inactivity.	☐ Yes ☐ Partial ☐ No	Configure 15-20 min timeout on all ePHI systems
Emergency Access	Required. Break-glass procedures needed.	No change but more documentation expected.	☐ Yes ☐ Partial ☐ No	Document and test break-glass procedures

Self-Assessment:

- ☐ Every user accessing ePHI has a unique, individual account (no shared logins)
- ☐ MFA is enabled for our EHR / primary clinical system
- ☐ MFA is enabled for email (Microsoft 365 / Google Workspace)
- ☐ MFA is enabled for VPN / remote access
- ☐ MFA is enabled for cloud applications that handle ePHI
- ☐ Session timeout is configured on all ePHI systems (15-20 minutes)
- ☐ We have a password policy that is technically enforced (not just written)
- ☐ We have documented break-glass (emergency access) procedures
- ☐ Access reviews are performed at least annually
- ☐ Terminated employees have access revoked within 24 hours across all systems

4. Audit Controls, Vulnerability Management & Testing

§164.312(b) — Audit Controls | Vulnerability Scanning & Pen Testing: CURRENT: Not explicit | PROPOSED: Required

Control Area	Current Requirement	Proposed Change	Your Status	Action Needed
Audit Logging	Required. Record and examine system activity.	More prescriptive. Must cover all ePHI systems with centralized logging.	☐ Yes ☐ Partial ☐ No	Enable logging on all ePHI systems; deploy central log management
Log Review	Required. Regular review of audit logs.	Must be documented with evidence of regular review cadence.	☐ Yes ☐ Partial ☐ No	Establish scheduled log review with documented findings
Vulnerability Scanning	Not explicitly required	Mandatory. Biannual vulnerability scans of all ePHI systems.	☐ Yes ☐ Partial ☐ No	Deploy scanner; scan every 6 months minimum; track remediation
Penetration Testing	Not explicitly required	Mandatory. Annual penetration testing.	☐ Yes ☐ Partial ☐ No	Budget for and schedule annual third-party pen test
Patch Management	Not explicitly required	Written patch management policies and procedures required.	☐ Yes ☐ Partial ☐ No	Establish patch policy with remediation timelines

Self-Assessment:

- ☐ Audit logging is enabled on ALL systems that store or access ePHI
- ☐ Logs are forwarded to a central system (SIEM or log aggregator)
- ☐ Log reviews are performed on a documented schedule (not ad-hoc)
- ☐ We have performed a vulnerability scan within the past 6 months
- ☐ Vulnerability scan findings have documented remediation timelines
- ☐ We have performed a penetration test within the past 12 months
- ☐ Pen test findings have been remediated or have documented risk acceptance
- ☐ We have a written patch management policy
- ☐ Critical patches are applied within a defined SLA (e.g., 30 days)

5. Incident Response & Contingency Planning

§164.308(a)(6) and §164.308(a)(7) — Security Incident Procedures / Contingency Plan | 72-Hr Restoration: PROPOSED: Required

Control Area	Current Requirement	Proposed Change	Your Status	Action Needed
Incident Response	Required. Identify, respond to, mitigate, and document incidents.	No fundamental change but higher documentation standard expected.	☐ Yes ☐ Partial ☐ No	Written IR plan with defined roles, escalation, and notification
Data Backup	Required. Maintain retrievable copies of ePHI.	Must demonstrate tested backup and verified restoration capability.	☐ Yes ☐ Partial ☐ No	Verify backups; TEST restoration regularly
Disaster Recovery	Required. Procedures to restore lost data.	72-hour restoration requirement for critical ePHI systems.	☐ Yes ☐ Partial ☐ No	Test DR against 72-hour SLA; document results
Emergency Operations	Required. Continue critical processes during emergency.	Must include ransomware and extended outage scenarios.	☐ Yes ☐ Partial ☐ No	Document manual/downtime procedures for EHR outage

Self-Assessment:

- ☐ We have a written Incident Response Plan
- ☐ The IR plan defines what constitutes a security incident
- ☐ Staff know how to report a suspected security incident
- ☐ We have conducted a tabletop exercise or IR drill within the past 12 months
- ☐ Backups cover ALL systems containing ePHI
- ☐ Backups are encrypted
- ☐ Backup restoration has been TESTED within the past 12 months
- ☐ We can restore critical ePHI systems within 72 hours (verified by test)
- ☐ We have documented manual/downtime procedures for EHR access during outages
- ☐ We have a communication plan for notifying affected parties during an incident

6. Physical Security, Workforce & Business Associates

§164.310, §164.308(a)(3), §164.308(b) — Physical Safeguards / Workforce Security / BA Contracts

Control Area	Current Requirement	Proposed Change	Your Status	Action Needed
Facility Security	Addressable. Facility security plan, access controls, visitor logs.	Mandatory. All physical access controls become required.	☐ Yes ☐ Partial ☐ No	Server room access restricted and logged; visitor procedures
Device Controls	Disposal and media re-use Required. Accountability Addressable.	All mandatory. Full hardware lifecycle tracking required.	☐ Yes ☐ Partial ☐ No	Track all devices; secure disposal with certificates
Workforce Training	Addressable. Security awareness training.	Mandatory. Regular training with documented completion.	☐ Yes ☐ Partial ☐ No	Annual security training for all workforce members
Termination	Addressable. Procedures for revoking access.	Mandatory. Documented termination procedures.	☐ Yes ☐ Partial ☐ No	Checklist covering all systems; verify no orphaned accounts
BA Agreements	Required. Written BAAs with all business associates.	BAAs directly liable. Stricter verification requirements.	☐ Yes ☐ Partial ☐ No	Audit BA inventory; verify current BAAs for all vendors

Self-Assessment:

- ☐ Server rooms and network closets have restricted, logged access
- ☐ Visitor sign-in procedures are enforced at all facilities
- ☐ Security cameras are functioning and footage is retained per policy
- ☐ All workforce members have completed security awareness training this year
- ☐ We have a termination checklist that covers all ePHI system access revocation
- ☐ Hardware disposal includes documented secure wiping or destruction
- ☐ We maintain a complete inventory of all business associates who handle ePHI
- ☐ Current, executed BAAs are on file for every business associate
- ☐ We have verified that BAAs include required provisions (breach notification, subcontractors)

Summary Scorecard

Tally your results from each section. For each control area, assess your overall readiness and identify the areas that require the most urgent attention.

Control Area	Ready	Partial	Not Ready	Priority Level	Notes / Next Steps
1. Security Risk Assessment	■	■	■	■ Critical ■ High ■ Medium ■ Low	
2. Encryption (At Rest)	■	■	■	■ Critical ■ High ■ Medium ■ Low	
2. Encryption (In Transit)	■	■	■	■ Critical ■ High ■ Medium ■ Low	
3. Multi-Factor Authentication	■	■	■	■ Critical ■ High ■ Medium ■ Low	
3. Access Controls	■	■	■	■ Critical ■ High ■ Medium ■ Low	
4. Audit Logging & Monitoring	■	■	■	■ Critical ■ High ■ Medium ■ Low	
4. Vulnerability Scanning	■	■	■	■ Critical ■ High ■ Medium ■ Low	
4. Penetration Testing	■	■	■	■ Critical ■ High ■ Medium ■ Low	
5. Incident Response Plan	■	■	■	■ Critical ■ High ■ Medium ■ Low	
5. Backup & Disaster Recovery	■	■	■	■ Critical ■ High ■ Medium ■ Low	
5. 72-Hour Restoration	■	■	■	■ Critical ■ High ■ Medium ■ Low	
6. Physical Security	■	■	■	■ Critical ■ High ■ Medium ■ Low	

Control Area	Ready	Partial	Not Ready	Priority Level	Notes / Next Steps
6. Workforce Training	☒	☒	☒	☒ Critical ☐ ☒ High ☐ ☐ Medium ☐ Low	
6. Business Associate Agreements	☒	☒	☒	☒ Critical ☐ ☒ High ☐ ☐ Medium ☐ Low	

Interpreting Your Results: If you marked 'Not Ready' on items 1, 2, or 3 (Risk Assessment, Encryption, or MFA), these should be your immediate priorities. They carry the highest enforcement risk under both the current and proposed rules. If you don't have a current Security Risk Assessment, that is your single most urgent action item — everything else flows from it.

What To Do Next

Step 1: Conduct a Security Risk Assessment. If you don't have one that's current, comprehensive, and tied to your technology asset inventory, this is your highest priority. It's the #1 thing OCR looks for, the #1 thing they fine for, and the foundation for everything else. The assessment should cover all Administrative, Physical, and Technical safeguards and produce a documented report you can keep on file.

Step 2: Close the critical gaps. Based on the assessment, prioritize encryption (at rest and in transit), MFA, and access controls. These are the areas with the highest enforcement risk and the ones that take the most time to implement. A risk-prioritized approach is what OCR expects to see.

Step 3: Establish an ongoing compliance program. The proposed rule requires annual assessments, biannual vulnerability scans, and annual penetration tests. This isn't a one-time project — it's an ongoing program. Build the cadence now so it's routine, not a scramble.

Need Help? We Do This Every Day.

Sidechain Security has spent 8 years helping healthcare organizations in the Pacific Northwest navigate security and compliance challenges. We specialize in performing the comprehensive HIPAA Security Risk Assessments that OCR requires — and our core expertise is encryption, the single biggest change in the proposed rule.

Trusted by Premera Blue Cross, Delta Dental, US-RX Care, and healthcare organizations across Oregon and Washington.

✉ info@sidechainsecurity.com | 🌐 sidechainsecurity.com | 📍 Portland, Oregon

Book a free 20-minute consultation to discuss where your organization stands and what to prioritize.

This checklist is provided for informational purposes and does not constitute legal advice. Organizations should consult with qualified legal and compliance professionals regarding their specific HIPAA obligations. Information is current as of May 2026.