Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

COMPLIANCE CHECKLIST — COVERED ENTITIES & BUSINESS ASSOCIATES

HIPAA Security Rule Implementation Checklist

Required & Addressable Safeguards · Administrative · Physical · Technical

v1.0 — 2026

Axiom Sovereign LLC · Severna Park, MD · info@axiomsovereign.com · axiomsovereign.com

HIPAA Security Rule Implementation Checklist

About This Checklist

This checklist provides a comprehensive implementation guide for the HIPAA Security Rule (45 CFR Parts 160 and 164) for covered entities — medical groups, physician practices, hospitals, health plans, and their business associates. It is organized according to the three safeguard categories defined in the Security Rule: Administrative, Physical, and Technical, followed by organizational and policy requirements.

The HIPAA Security Rule establishes national standards for protecting electronic protected health information (ePHI). Every covered entity and business associate — including practice management vendors, billing companies, EHR providers, and AI tools that access patient data — must implement these requirements. The Office for Civil Rights (OCR) enforces the Security Rule with civil monetary penalties ranging from $100 to $50,000 per violation, with annual caps reaching $1.9 million per violation category.

This checklist incorporates updated OCR guidance issued in 2024, including the December 2024 HIPAA Security Rule NPRM that proposed mandatory implementation specifications for previously addressable requirements. Organizations should treat previously addressable specifications as effectively required in the current enforcement environment.

How to Read This Checklist

R = Required: Implementation is mandatory with no flexibility. Every covered entity must implement.

A = Addressable: Must either implement the specification OR document in writing why it is not reasonable and appropriate, and implement an equivalent alternative measure. In practice, most addressable specifications should be implemented — "not reasonable and appropriate" is a high bar that OCR scrutinizes heavily.

Status Column: Mark each item as Implemented (I), Partially Implemented (P), or Not Implemented (N). Items marked N require either immediate implementation or documented justification.

Methodology: How to Use This Checklist

This checklist is designed to be used in conjunction with a formal HIPAA Security Risk Analysis — the risk analysis required by 45 CFR §164.308(a)(1). The risk analysis identifies your specific threats and vulnerabilities; this checklist ensures the required safeguards are in place to address them. Neither document replaces the other.

Complete this checklist by walking through each safeguard with the individual responsible for your organization's IT systems and security controls. For each item marked "Addressable," if you have not implemented it, you must document your reasoning in a Risk Management Plan. OCR auditors will ask to see this documentation.

Step 1 — Convene the Right People: Complete this checklist with your IT administrator, practice administrator, and compliance officer together. No single person has complete visibility into all three safeguard areas.

Step 2 — Document Your Evidence: For each item marked Implemented, note the evidence of implementation in the Notes column — the name of the policy, the system configuration, or the vendor that provides the control. "Implemented" without evidence is not defensible in an OCR audit.

Step 3 — Create Your Gap List: Every item marked N or P goes on your remediation list with a responsible owner, target date, and budget estimate. This becomes your HIPAA Risk Management Plan.

Step 4 — Review Annually and After Significant Changes: The Security Rule requires periodic review. Review this checklist annually and whenever you add new ePHI systems, change vendors, adopt new AI tools, or experience a workforce change affecting access to ePHI.

ADMINISTRATIVE SAFEGUARDS (45 CFR 164.308)

Administrative safeguards are the policies, procedures, and management processes that protect ePHI and guide workforce conduct with respect to ePHI. They are the largest and most complex category of HIPAA Security Rule requirements, comprising the majority of OCR enforcement actions.

CFR Ref.	Safeguard / Requirement	R/A	Implementation Guidance	Status (I/P/N)	Notes & Evidence
164.308(a)(1)(ii)(A)	Risk Analysis — Conduct an accurate and thorough assessment of potential risks and vulnerabilities to ePHI.	R	Must be documented, address all ePHI systems, quantify likelihood and impact of threats, and be updated when significant changes occur. This is the most-cited HIPAA violation in OCR audits.		
164.308(a)(1)(ii)(B)	Risk Management — Implement security measures to reduce risks to ePHI to a reasonable and appropriate level.	R	A documented Risk Management Plan must address each risk identified in the Risk Analysis with a specific control, owner, and target date. Standalone risk analysis without a management plan is insufficient.		
164.308(a)(1)(ii)(C)	Sanction Policy — Apply appropriate sanctions against workforce members who violate security policies.	R	Must be written, communicated to all staff, and consistently applied. Document all sanctions applied. Inconsistent enforcement undermines the entire policy structure.		
164.308(a)(1)(ii)(D)	Information System Activity Review — Regularly review audit logs, access reports, and security incident tracking reports.	R	Define the review frequency (weekly for high-risk systems, monthly minimum), who performs the review, and what constitutes a reportable anomaly. Document reviews performed.		
164.308(a)(2)	Assigned Security Responsibility — Designate a security official responsible for policies and procedures.	R	Must be a named individual, not a role or department. For small practices, this may be the physician owner or practice manager. For larger organizations, this should be a dedicated security or compliance officer.		

CFR Ref.	Safeguard / Requirement	R/A	Implementation Guidance	Status (I/P/N)	Notes & Evidence
164.308(a)(3)	Workforce Authorization and Supervision — Implement procedures for authorization/supervision of workforce members.	R	Include: background check requirements, role-based access authorization, supervision requirements for members who work with ePHI, and clearance procedures for termination.		
164.308(a)(4)	Information Access Management — Implement policies for authorizing access to ePHI.	R	Define who can access which ePHI, the process for granting access, how access is modified when roles change, and how access is terminated when employment ends.		
164.308(a)(5)	Security Awareness and Training — Train all workforce members on security policies and procedures.	R (implementation specs are A)	Training must be completed by all staff, documented with individual completion records, and updated when policies change. Include: phishing recognition, password security, AI tool governance, incident reporting.		
164.308(a)(6)	Security Incident Procedures — Identify, respond to, and document suspected or known security incidents.	R	Must include: identification procedures, reporting mechanisms, response steps, mitigation actions, and post-incident documentation. Define what constitutes an incident vs. a breach.		
164.308(a)(7)	Contingency Plan — Data backup, disaster recovery, and emergency mode operation plans.	R	Five components required: data backup plan, disaster recovery plan, emergency mode operation plan, testing and revision procedures, applications and data criticality analysis.		
164.308(b)	Business Associate Agreements (BAAs) — Written agreements with all business associates.	R	BAA required with EVERY vendor that creates, receives, maintains, or transmits ePHI on your behalf — including EHR vendors, billing services, cloud storage, transcription services, and AI tools that access patient data.		

PHYSICAL SAFEGUARDS (45 CFR 164.310)

Physical safeguards protect electronic information systems, buildings, and equipment from unauthorized physical access, tampering, and theft. For small and mid-size practices, these requirements are often the most straightforward to implement — but are frequently underdocumented.

CFR Ref.	Safeguard / Requirement	R/A	Implementation Guidance	Status (I/P/N)	Notes & Evidence
164.310(a)(1)	Facility Access Controls — Limit physical access to electronic information systems and the facilities in which they are housed.	A	Implement for server rooms, data centers, workstation areas with ePHI, and any physical location where ePHI is stored or accessed. May include locked server rooms, badge access, visitor logs.		
164.310(a)(2)(ii)	Contingency Operations — Establish procedures for ePHI access during emergency operations.	A	Align with your disaster recovery plan. Define who can access which systems during emergencies, how access is granted when normal authentication is unavailable, and how emergency access is documented.		
164.310(a)(2)(iii)	Facility Security Plan — Implement policies to safeguard facilities with ePHI from unauthorized physical access.	A	May include: security cameras, alarm systems, physical access controls, clean desk policy, and visitor management procedures. Document the plan and review annually.		
164.310(b)	Workstation Use — Specify the proper functions performed on workstations that access ePHI.	R	Document: which workstations may access ePHI, what functions may be performed, physical environment requirements (screen placement, locking when unattended), and personal use restrictions.		
164.310(c)	Workstation Security — Implement physical safeguards for workstations that access ePHI.	R	Covers all workstations — desktops, laptops, tablets, and workstations in public or semi-public areas. Include requirements for screen locks, cable locks for portable devices, and clean desk policies.		

CFR Ref.	Safeguard / Requirement	R/A	Implementation Guidance	Status (I/P/N)	Notes & Evidence
164.310(d)(1)	Device and Media Controls — Govern the receipt, removal, backup, and disposal of hardware and electronic media containing ePHI.	R	Must address: final disposal of hardware (data destruction documentation), re-use of media (secure wiping), accountability tracking for hardware containing ePHI, and data backup before movement.		
164.310(d)(2)(iv)	Encryption — Encrypt ePHI on portable devices and removable media.	A	OCR treats encryption of portable devices as effectively required — unencrypted laptop breach = automatic notification. NIST recommends AES-256 minimum. Document devices that cannot be encrypted and why.		

TECHNICAL SAFEGUARDS (45 CFR 164.312)

Technical safeguards are the technology-based controls that protect ePHI and control access to it. This section has seen the most significant evolution in OCR guidance as technology has changed — particularly around multi-factor authentication and AI tool governance.

CFR Ref.	Safeguard / Requirement	R/A	Implementation Guidance	Status (I/P/N)	Notes & Evidence
164.312(a)(1)	Access Control — Unique user identification, emergency access, automatic logoff, encryption.	R (core) A (specs)	Unique user IDs are required — shared accounts are not permitted. Emergency access procedures must be defined. Automatic logoff after inactivity (15 minutes recommended for ePHI systems).		
164.312(a)(2)(iv)	Encryption of ePHI at Rest — Encrypt ePHI stored in information systems.	A	Encrypt all databases, file shares, and storage systems containing ePHI. Cloud-based ePHI must be encrypted using keys you control or keys controlled by a business associate under BAA. AES-256 minimum.		
164.312(b)	Audit Controls — Hardware, software, and procedural mechanisms to record and examine activity in information systems with ePHI.	R	Enable and retain audit logs for all systems with ePHI: login/logout events, ePHI access, failed login attempts, administrative actions. Retain logs for minimum 6 years. Review logs regularly (see 164.308(a)(1)(ii)(D)).		
164.312(c)(1)	Integrity — Protect ePHI from improper alteration or destruction.	R (core) A (spec)	Implement mechanisms to ensure ePHI has not been altered or destroyed without authorization. Includes: hash verification, version control, access controls that prevent unauthorized modification.		
164.312(d)	Authentication — Verify the identity of persons or entities seeking access to ePHI.	R	Implement multi-factor authentication (MFA) for all ePHI system access. OCR's 2024 NPRM proposed making MFA a required specification. Current enforcement environment treats MFA as effectively required.		

CFR Ref.	Safeguard / Requirement	R/A	Implementation Guidance	Status (I/P/N)	Notes & Evidence
164.312(e)(1)	Transmission Security — Guard against unauthorized access to ePHI transmitted over networks.	R (core) A (spec)	All ePHI transmitted over open networks must be protected. TLS 1.2 or higher for web portals and APIs. VPN for remote access. Email encryption for messages containing ePHI (not standard email).		
164.312(e)(2)(ii)	Encryption of ePHI in Transit	A	Encrypt all ePHI transmitted over open networks. Use TLS 1.3 where possible. Do not transmit ePHI via standard unencrypted email. Use secure patient portals or encrypted messaging for patient communication.		
AI Tools — 2024 OCR Guidance	AI Tools Accessing ePHI — Execute BAAs with all AI vendors that access, process, or store ePHI.	R	AI transcription tools, clinical AI, AI-assisted coding, and any AI that processes patient records requires a BAA. Verify the AI vendor will execute a BAA. Vendors who refuse cannot be used with ePHI.		

ORGANIZATIONAL REQUIREMENTS AND DOCUMENTATION

CFR Ref.	Requirement	R/A	Implementation Guidance	Status (I/P/N)	Notes & Evidence
164.520	Notice of Privacy Practices (NPP) — Provide to patients at first service delivery.	R	NPP must describe how PHI is used and disclosed, patient rights, and how to file complaints. Must be posted in the facility and on your website. Update when practices change.		
164.400–414	Breach Notification — Notify individuals, HHS, and media (if 500+ affected) of unsecured PHI breaches.	R	Individual notification required within 60 days of discovery. HHS notification within 60 days. Media notification within 60 days if 500+ residents of a state affected. Maintain breach log.		
164.530(b)	Training Documentation — Document all workforce training.	R	Record: training date, content covered, trainer or training system, and individual completion with signature or electronic acknowledgment. Retain for 6 years.		
164.316	Policy and Procedure Documentation — Document all policies and procedures.	R	All Security Rule policies must be in writing. Retain documentation for 6 years from creation or last effective date. Implement version control and review cycle.		
164.308(a)(8)	Evaluation — Perform a periodic technical and nontechnical evaluation.	R	Conduct evaluation when environmental or operational changes affect ePHI security. Annual evaluation is the standard. Document findings and any resulting policy changes.		

COMPLIANCE SUMMARY AND NEXT STEPS

Administrative Safeguards Implemented: _____ / 12

Physical Safeguards Implemented: _____ / 7

Technical Safeguards Implemented: _____ / 8

Organizational Requirements Implemented: _____ / 5

TOTAL IMPLEMENTED: _____ / 32

Items requiring immediate remediation (Not Implemented — Required specifications):

_____

_____

_____

HIPAA Implementation Support

Axiom Sovereign implements HIPAA Security Rule programs for medical groups and healthcare practices — completing your risk analysis, authoring required policies, configuring technical safeguards, executing BAAs with AI and technology vendors, delivering staff training, and managing ongoing compliance. Our HIPAA engagement begins with a gap assessment and delivers a complete, auditable program.

Schedule a complimentary HIPAA readiness review: calendly.com/cmissimore-62kc/30min

Email: info@axiomsovereign.com · **Web:** axiomsovereign.com