HIPAA AUDITORS

Security Management Process Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.308(a)(1) — Security Management Process

Issued	9 August 2026
Prepared by	HIPAA Auditors — certified HIPAA lead auditors
Contact	info@hipaaauditors.com · +91-95851-60363
Address	100 Congress Ave, Suite 2000, Austin, TX 78701

How to use this document. This is a working template, not a finished compliance artefact. Replace every bracketed placeholder with your organisation’s own detail, delete the guidance notes, and have the result reviewed and formally adopted by your Privacy or Security Officer before you rely on it.

Regulatory basis. References are to the HIPAA Administrative Simplification regulations at 45 CFR Parts 160, 162 and 164, and to NIST SP 800-66 Rev. 2, *Implementing the HIPAA Security Rule*.

The requirement

Implement policies and procedures to prevent, detect, contain, and correct security violations.

45 CFR 164.308(a)(1) · Administrative Safeguards

Risk level	Difficulty	Typical cost	Timeframe
Critical	Complex	High	3-6 months

Implementation steps

	Implement policies and procedures to prevent, detect, contain and correct security violations. This is the foundational standard of the Security Rule: the four specifications beneath it drive every other safeguard decision you make, and all four are Required — none is addressable
	Required implementation specifications:
	Risk analysis — 164.308(a)(1)(ii)(A). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of all ePHI you hold. This is the single most frequently cited failure in OCR enforcement. It must cover the whole ePHI estate, not a sample, and it must be documented and dated
	Risk management — 164.308(a)(1)(ii)(B). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. The analysis identifies risk; risk management is what you do about it, prioritised by the ratings you assigned
	Sanction policy — 164.308(a)(1)(ii)(C). Apply appropriate sanctions against workforce members who fail to comply with your security policies and procedures. It must exist, be communicated, and be applied consistently — selective enforcement undermines it entirely
	Information system activity review — 164.308(a)(1)(ii)(D). Regularly review records of information system activity: audit logs, access reports and security incident tracking reports. This pairs directly with the audit controls standard at 164.312(b), which provides the records this specification requires you to examine
	Implementation approach:
	- Scope the risk analysis to every system, device, medium, facility and third party that creates, receives, maintains or transmits ePHI, then diagram the data flows
	- Rate risks on a documented, reproducible scale of likelihood and impact, and publish the scale
	- Feed every identified risk into a tracked remediation plan with an owner and a date, and record accepted risks with the reasoning
	- Update the analysis on material change — new systems, mergers, new premises, significant incidents — rather than only annually
	- Make activity review a scheduled task with a named owner and a written record of what was examined

- [ ] **- Apply the sanction policy visibly and record every application, including the decision not to sanction**
- [ ] **A vulnerability scan is not a risk analysis. A scan enumerates technical weaknesses in the systems it was pointed at; a risk analysis covers the whole estate, includes non-technical vulnerabilities such as absent policy or untrained staff, and rates the risk each presents. Submitting a scan report in place of an analysis is a recurring enforcement finding**

Evidence to produce and retain

Tick only where the artefact exists and you can say where it lives.

- [ ] **Security management process policy and supporting procedures**
  Location: _____ Owner: _____
- [ ] **Risk analysis report: scope, methodology, asset and data flow inventory, threats, vulnerabilities, current controls, likelihood and impact ratings, and risk determinations**
  Location: _____ Owner: _____
- [ ] **Documented likelihood and impact rating scales**
  Location: _____ Owner: _____
- [ ] **Risk management plan with owners, priorities and target dates**
  Location: _____ Owner: _____
- [ ] **Risk acceptance records, with the reasoning and the approver**
  Location: _____ Owner: _____
- [ ] **Sanction policy, evidence of communication to the workforce, and records of application**
  Location: _____ Owner: _____
- [ ] **Information system activity review procedure naming reviewer, scope and frequency**
  Location: _____ Owner: _____
- [ ] **Completed activity review records showing what was examined and what was found**
  Location: _____ Owner: _____
- [ ] **Evidence of risk analysis updates following material change**
  Location: _____ Owner: _____
- [ ] **Approval and version history for each document**
  Location: _____ Owner: _____

How this gets tested

These are the procedures an auditor is likely to run. Self-test first.

- [ ] **Confirm a documented, dated risk analysis exists and covers the entire ePHI estate rather than a subset**
  Result: _____ Tested by / date: _____

	Compare the risk analysis asset inventory against an independently compiled system list to test completeness Result: _____ Tested by / date: _____
	Confirm the analysis includes non-technical vulnerabilities, not only scan output Result: _____ Tested by / date: _____
	Verify likelihood and impact scales are documented and applied consistently Result: _____ Tested by / date: _____
	Trace a sample of identified risks into the risk management plan and confirm owners and dates Result: _____ Tested by / date: _____
	Confirm remediation priority follows risk rating rather than convenience Result: _____ Tested by / date: _____
	Review risk acceptance records for reasoning and appropriate approval Result: _____ Tested by / date: _____
	Confirm the sanction policy exists, was communicated, and has been applied consistently where breaches occurred Result: _____ Tested by / date: _____
	Inspect activity review records and confirm they show substance, not just attestation Result: _____ Tested by / date: _____
	Confirm the analysis was updated after recent material changes or incidents Result: _____ Tested by / date: _____

Common failures to check yourself against

- No risk analysis at all, or one so narrow it omits whole systems — the most cited HIPAA failure
- A vulnerability scan report submitted in place of a risk analysis
- Risk analysis performed but never documented, or undated
- Risks identified and then never tracked to remediation
- Remediation ordered by ease rather than by risk rating
- Sanction policy absent, or present but never applied
- Sanctions applied inconsistently, undermining the policy
- Information system activity review never performed, or performed with no record
- Analysis never updated after mergers, new systems or major incidents
- Accepted risks left implicit, with no reasoning or approver recorded

Beyond the minimum

- Treat the risk analysis as a living document tied to change control, not an annual project
- Diagram ePHI data flows; a written asset list alone consistently misses transmission paths
- Publish your rating scales so risk determinations are reproducible and challengeable
- Track remediation in the same system used for other operational work so it stays visible
- Record accepted risks explicitly, with a named approver, rather than leaving them unaddressed

- Automate activity review detection, then evidence the human review that follows
- Apply the sanction policy consistently and document every application
- Report risk posture to leadership regularly so remediation is resourced
- Re-run the analysis after mergers, new premises, major system changes and significant incidents

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.1.1; NIST SP 800-30 Rev. 1 (Risk Assessment); NIST SP 800-37 Rev. 2 (Risk Management Framework)

Sign-off

Completed by	Title	Date
Reviewed by	**Title**	**Next review due**