HIPAA AUDITORS

Policies and Procedures Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.316(a) — Policies and Procedures

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 reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart.

45 CFR 164.316(a) · Policies and Procedures

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

Implementation steps

	Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of the Security Rule, taking into account the factors at 164.306(b)(2). A covered entity or business associate may change its policies and procedures at any time, provided the changes are documented and implemented in line with 164.316
	Policies must map to the rule and to your own environment. A purchased template adopted without tailoring is a recurring finding, because the policy describes controls the organisation does not operate — which is worse than an acknowledged gap, since it evidences a failure to know your own environment
	Implementation approach:
	Build a policy set that covers every standard and addressable specification, and record where each is addressed
	Distinguish policy from procedure: policy states what and why; procedure states who, how and how often. Auditors ask for both, and organisations most often have only the first
	Tailor to your systems, size, complexity and the risk analysis findings. The 164.306(b)(2) factors — size and capability, technical infrastructure, cost, and the probability and criticality of risks — are the stated basis for reasonableness
	Have each policy formally approved by the Security Officer or an authorised body, with the approval dated
	Version every document, and keep superseded versions; you must be able to show what was in force at any past date
	Distribute so the workforce can actually reach the current version, and record acknowledgement
	Review at least annually, and on any material change to operations, technology or regulation. Record the review even when nothing changes — an undated policy is treated as unmaintained
	Where a policy exists but is not followed, you hold documented evidence of your own non-compliance; fix the practice or fix the policy

- [ ] **coverage, and it makes gaps visible to you before they are visible to a regulator**

  Maintain a control-to-policy matrix. It is the single most useful artefact for demonstrating

Evidence to produce and retain

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

- [ ] **Complete policy and procedure set covering every Security Rule standard and specification**
  Location: _____ Owner: _____
- [ ] **Control-to-policy matrix mapping each requirement to the document addressing it**
  Location: _____ Owner: _____
- [ ] **Documented decisions for every addressable specification, including equivalent alternatives**
  Location: _____ Owner: _____
- [ ] **Approval records showing approver, role and date for each document**
  Location: _____ Owner: _____
- [ ] **Version history, with superseded versions retained**
  Location: _____ Owner: _____
- [ ] **Distribution and workforce acknowledgement records**
  Location: _____ Owner: _____
- [ ] **Annual review records, including reviews that resulted in no change**
  Location: _____ Owner: _____
- [ ] **Change log capturing what changed, why, and when it took effect**
  Location: _____ Owner: _____
- [ ] **Evidence that procedures reflect actual operating practice**
  Location: _____ Owner: _____
- [ ] **Retention evidence meeting the six-year requirement at 164.316(b)(2)**
  Location: _____ Owner: _____

How this gets tested

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

- [ ] **Compare the policy set against every Security Rule standard and specification to identify gaps**
  Result: _____ Tested by / date: _____
- [ ] **Confirm each addressable specification has a documented decision, not silence**
  Result: _____ Tested by / date: _____
- [ ] **Check that every document carries an owner, approval date and version**
  Result: _____ Tested by / date: _____
- [ ]

	Result: _____ Tested by / date: _____
	Sample staff and confirm they actually locate the documented procedure Result: _____ Tested by / date: _____
	Confirm review dates are current and that reviews are evidenced even where nothing changed Result: _____ Tested by / date: _____
	Confirm workforce acknowledgement records exist and cover current staff Result: _____ Tested by / date: _____
	Retrieve a superseded version to confirm historic versions are retained and identifiable Result: _____ Tested by / date: _____
	Verify the policies reflect this organisation's systems rather than generic template content Result: _____ Tested by / date: _____
	Trace a recent operational change through to the policy update it should have triggered Result: _____ Tested by / date: _____

Common failures to check yourself against

- Purchased templates adopted verbatim, describing controls the organisation does not operate
- Policies present with no corresponding procedures, so nobody knows who does what
- Documents with no approval date, owner or version
- No review for several years, leaving policies describing retired systems
- Addressable specifications passed over with no documented decision
- Policies that contradict observed practice, evidencing non-compliance in the organisation's own records
- Superseded versions discarded, making it impossible to show what was in force historically
- No workforce acknowledgement records
- Whole standards unaddressed because no coverage mapping exists

Beyond the minimum

- Maintain a control-to-policy matrix so coverage and gaps are both visible
- Write procedures that name the responsible role and the frequency, so they are testable
- Tailor every document to your actual systems; generic templates produce findings
- Version and date everything, and retain superseded copies
- Review annually on a schedule, and record the review even when unchanged
- Tie policy updates to change control so operational changes trigger document updates
- Capture workforce acknowledgement at induction and after material revisions
- Record the reasoning for addressable specifications inside or alongside the relevant policy
- Keep documents readable; policies nobody can follow are not implemented in practice

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.5.1

Sign-off

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

Want this verified independently? We test controls like this one on every HIPAA engagement. Request a scoped quote at https://hipaaauditors.com/contact