HIPAA AUDITORS

Documentation Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.316(b)(1) — Documentation

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

Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form.

45 CFR 164.316(b)(1) · Policies and Procedures

Risk level	Difficulty	Typical cost	Timeframe
High	Moderate	Medium	2-4 months

Implementation steps

	Maintain the policies and procedures implemented to comply with this subpart in written form, which may be electronic. Where an action, activity or assessment is required to be documented, maintain a written record of it
	The second half is where organisations fail. Policies are usually written; the record of the required activities frequently is not. Under the Security Rule the evidence effectively is the compliance — an activity you cannot evidence is treated as an activity that did not happen
	Documentation must cover:
	Policies and procedures for every standard and implementation specification
	The risk analysis and risk management decisions, including accepted risks and why
	Decisions on every addressable specification, with equivalent alternatives where applicable
	Security incidents, their investigation and their outcomes
	Workforce training delivery, attendance and content version
	Sanctions applied under the sanction policy
	Information system activity reviews, including what was examined and what was found
	Periodic evaluations under 164.308(a)(8)
	Access authorisations, modifications and terminations
	Business associate agreements and related assurances
	Contingency plan testing and revision
	Facility access and maintenance records
	Implementation approach:
	- Assign an owner to each documentation type; unowned records are the ones that stop being kept
	- Define where each record lives, so it can be produced quickly under time pressure

	reconstructed and damages credibility
	- Protect documentation integrity so that activity can be reconstructed evidence is visibly
	- Index the set so a regulator request can be answered in days rather than weeks
	- Apply the six-year retention rule at 164.316(b)(2) consistently
	- Include electronic evidence such as configuration exports, log extracts and ticket records
	OCR investigations routinely begin with a documentation request. The speed and completeness of that response shapes everything that follows

Evidence to produce and retain

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

	Complete written policy and procedure set, electronic form acceptable Location: _____ Owner: _____
	Documentation inventory listing each required record, its owner and its location Location: _____ Owner: _____
	Risk analysis reports and risk management decision records Location: _____ Owner: _____
	Addressable specification decision records Location: _____ Owner: _____
	Security incident files, including investigation and resolution Location: _____ Owner: _____
	Training records with dates, attendees and material version Location: _____ Owner: _____
	Sanction records where policy was breached Location: _____ Owner: _____
	Information system activity review records Location: _____ Owner: _____
	Periodic evaluation reports under 164.308(a)(8) Location: _____ Owner: _____
	Access authorisation, modification and termination records Location: _____ Owner: _____
	Business associate agreements and due diligence evidence Location: _____ Owner: _____
	Contingency plan test results and revisions Location: _____ Owner: _____

- [ ] Location: _____ Owner: _____

Retention and disposal schedule aligned to 164.316(b)(2)

How this gets tested

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

- [ ] **Request the documentation inventory and confirm each required record type is listed with an owner**
  Result: _____ Tested by / date: _____
- [ ] **Sample each record type and confirm it exists, is dated and is retrievable**
  Result: _____ Tested by / date: _____
- [ ] **Test retrieval speed by requesting a specific historic record without notice**
  Result: _____ Tested by / date: _____
- [ ] **Confirm records are timestamped contemporaneously rather than assembled retrospectively**
  Result: _____ Tested by / date: _____
- [ ] **Verify the risk analysis is documented, dated and covers the whole ePHI estate**
  Result: _____ Tested by / date: _____
- [ ] **Confirm addressable specification decisions are recorded in writing**
  Result: _____ Tested by / date: _____
- [ ] **Check training records reconcile against the current staff list**
  Result: _____ Tested by / date: _____
- [ ] **Confirm activity review records show what was examined, not merely that review occurred**
  Result: _____ Tested by / date: _____
- [ ] **Verify retention meets six years by retrieving a record from the earliest period**
  Result: _____ Tested by / date: _____
- [ ] **Confirm documentation integrity controls prevent undetected alteration**
  Result: _____ Tested by / date: _____

Common failures to check yourself against

- Policies documented but required activities not evidenced
- Risk analysis performed but never written up, or written up without a date
- Training delivered with no attendance record
- Activity reviews claimed but with no record of what was examined
- Addressable specification decisions never documented
- Records scattered across individuals' mailboxes and drives, unretrievable under pressure
- Evidence assembled after a regulator request, visibly reconstructed
- Retention shorter than six years, so historic evidence no longer exists
- No documentation owner, so record-keeping lapses unnoticed
- Sanctions applied but never recorded

Beyond the minimum

- Maintain a documentation inventory naming the owner and storage location for each record type
- Generate evidence as a by-product of the activity rather than as a separate later exercise
- Timestamp at the time of the activity; contemporaneous records carry far more weight
- Centralise compliance documentation in one indexed, access-controlled repository
- Automate collection where possible: log exports, configuration snapshots, ticket records
- Rehearse a regulator documentation request annually to find the gaps before OCR does
- Restrict who can alter compliance records, and log changes
- Align retention and disposal to the six-year rule with a written schedule
- Keep the index current so any record can be produced within days

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.5.2

Sign-off

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