HIPAA AUDITORS

Time Limit Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.316(b)(2) — Time Limit

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

Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

45 CFR 164.316(b)(2) · Policies and Procedures

Risk level	Difficulty	Typical cost	Timeframe
Medium	Moderate	Medium	1-3 months

Implementation steps

	Retain the documentation required by 164.316(b)(1) for six years from the date of its creation or the date when it last was in effect, whichever is later. Make it available to those responsible for implementing the procedures, and review it periodically, updating as needed in response to environmental or operational changes affecting the security of ePHI
	The "whichever is later" clause is regularly misread. A policy in force for eight years must be retained for six years after it ceases to be in effect — fourteen years from creation in total. Retention schedules built on creation date alone delete evidence that is still required
	Note also that this six-year period is a federal floor, not a ceiling. State law, professional licensure requirements and medical record retention rules frequently demand longer, and the longest applicable period governs. HIPAA sets no medical record retention period at all; that is a matter of state law, and conflating the two is a common error
	Implementation approach:
	Build a retention schedule covering every documentation type, with the retention trigger stated
	Compute retention from the later of creation or last effective date, and record both
	Retain superseded policy versions for six years after they cease to apply
	Suspend disposal on litigation hold or regulatory inquiry, and document the suspension
	Prevent premature deletion technically, not only by policy — retention locks or immutable storage
	Preserve readability across format and system changes; six-year-old evidence must still open
	Assign a documentation owner responsible for the schedule
	Reconcile against state and professional requirements and apply the longest period
	Dispose securely at end of life, and record what was destroyed and when
	Review the schedule annually alongside the policy review cycle

Evidence to produce and retain

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

- [ ] **Retention schedule covering every documentation type and its retention trigger**
  Location: _____ Owner: _____
- [ ] **Records showing both creation date and last-effective date for each policy version**
  Location: _____ Owner: _____
- [ ] **Superseded policy and procedure versions within their retention window**
  Location: _____ Owner: _____
- [ ] **Retention configuration evidence, such as retention locks or immutable storage settings**
  Location: _____ Owner: _____
- [ ] **Legal hold and inquiry suspension records**
  Location: _____ Owner: _____
- [ ] **Format migration records demonstrating continued readability**
  Location: _____ Owner: _____
- [ ] **Secure disposal certificates and destruction logs**
  Location: _____ Owner: _____
- [ ] **Analysis reconciling HIPAA retention with state and professional requirements**
  Location: _____ Owner: _____
- [ ] **Annual retention schedule review records**
  Location: _____ Owner: _____
- [ ] **Named documentation owner and their responsibilities**
  Location: _____ Owner: _____

How this gets tested

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

- [ ] **Review the retention schedule and confirm it computes from the later of creation or last effective date**
  Result: _____ Tested by / date: _____
- [ ] **Retrieve a document from the earliest retained period and confirm it opens and is legible**
  Result: _____ Tested by / date: _____
- [ ] **Confirm superseded policy versions are retained with their effective and end dates recorded**
  Result: _____ Tested by / date: _____
- [ ] **Attempt to delete a record within its retention window and confirm prevention**
  Result: _____ Tested by / date: _____
- [ ] **Verify legal hold suspends disposal, and that suspensions are documented**
  Result: _____ Tested by / date: _____
- [ ]

	Sample disposal records and confirm items were genuinely eligible for destruction Result: _____ Tested by / date: _____
	Confirm destruction certificates exist for disposed records Result: _____ Tested by / date: _____
	Check the schedule against applicable state retention requirements Result: _____ Tested by / date: _____
	Confirm the schedule has been reviewed within the last year Result: _____ Tested by / date: _____
	Verify a named owner is accountable for retention Result: _____ Tested by / date: _____

Common failures to check yourself against

- Retention computed from creation date only, deleting evidence still within its window
- Superseded policy versions discarded on replacement
- Six years applied where state law requires longer
- No retention schedule, so practice varies by individual
- Retention unenforced technically, allowing premature deletion
- Legal hold not suspending routine disposal
- Old records retained but unreadable after a system or format change
- No destruction records for disposed documentation
- HIPAA's six-year documentation rule mistaken for a medical record retention period
- No named owner for retention

Beyond the minimum

- Record both creation and last-effective dates so the retention trigger can be computed correctly
- Enforce retention technically with immutable storage or retention locks, not policy alone
- Retain superseded versions for six years after they cease to apply, and label them clearly
- Automate legal hold so disposal stops immediately on notice
- Migrate formats proactively so old evidence remains readable
- Reconcile with state and professional retention rules and apply the longest period
- Keep destruction certificates; incomplete disposal records are themselves a finding
- Review the schedule annually with the policy review cycle
- Distinguish compliance documentation retention from medical record retention, which HIPAA does not govern

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.5.3

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