HIPAA AUDITORS

Audit Controls Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.312(b) — Audit Controls

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 hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

45 CFR 164.312(b) · Technical Safeguards

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

Implementation steps

	Implement hardware, software or procedural mechanisms that record and examine activity in systems containing or using ePHI. The standard has two halves, and organisations routinely satisfy only the first: you must record activity, and you must examine what you record
	What to record:
	Authentication events — successes, failures, lockouts and password changes
	Access to ePHI records, including read access, with the user, subject record, timestamp and source
	Creation, modification, deletion and export of ePHI
	Bulk queries, report generation, printing and downloads
	Privileged and administrative actions, including changes to accounts and permissions
	Changes to the audit configuration itself, and any attempt to disable or clear logs
	Remote access sessions, VPN connections and API activity
	What to do with it:
	- Define who reviews logs, how often, and what triggers escalation, then evidence that it happens
	- Automate detection for the patterns that matter: same-surname access, VIP record access, access outside working hours, bulk export, repeated authorisation failures
	- Centralise logs off the originating host so a compromised system cannot erase its own trail
	- Protect log integrity with append-only or write-once storage and restricted access
	- Set retention to at least six years where the log evidences compliance activity, per 164.316(b)(2)
	- Record each review: who reviewed, what period, what was found and what action followed
	Note the relationship with 164.308(a)(1)(ii)(D): the information system activity review specification requires regular review of audit logs, access reports and incident tracking reports. The two standards are tested together

Evidence to produce and retain

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

- [ ] **Audit controls policy defining what is logged, why, and for how long**
  Location: _____ Owner: _____
- [ ] **Log review procedure naming the reviewer role, frequency and escalation path**
  Location: _____ Owner: _____
- [ ] **Inventory of systems holding ePHI, each mapped to its logging configuration**
  Location: _____ Owner: _____
- [ ] **Audit log configuration evidence per system, including which event types are captured**
  Location: _____ Owner: _____
- [ ] **Completed log review records with reviewer, date, period covered, findings and actions**
  Location: _____ Owner: _____
- [ ] **Alert rule definitions and the tuning history behind them**
  Location: _____ Owner: _____
- [ ] **Log retention and protection standard, including integrity controls**
  Location: _____ Owner: _____
- [ ] **Records of any log-related incident and its investigation**
  Location: _____ Owner: _____
- [ ] **Evidence that audit configuration changes are themselves logged and approved**
  Location: _____ Owner: _____

How this gets tested

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

- [ ] **Confirm every system in the ePHI inventory produces logs, and identify any that do not**
  Result: _____ Tested by / date: _____
- [ ] **Verify read access to ePHI is captured, not only writes — this is the most common gap**
  Result: _____ Tested by / date: _____
- [ ] **Generate a test access event and confirm it appears in the log with user, record, timestamp and source**
  Result: _____ Tested by / date: _____
- [ ] **Attempt to modify or delete a log entry as a privileged user and confirm the attempt is prevented or recorded**
  Result: _____ Tested by / date: _____
- [ ]

	signature Result: _____ Tested by / date: _____
	Inspect a sample alert review triggered through investigation to confirm documentation rather than a Result: _____ Tested by / date: _____
	Confirm retention meets policy by retrieving a record from the earliest retained period Result: _____ Tested by / date: _____
	Check that clocks are synchronised across systems so events can be correlated Result: _____ Tested by / date: _____
	Verify logs are stored off the originating host and are access-restricted Result: _____ Tested by / date: _____
	Confirm audit configuration changes are logged and require approval Result: _____ Tested by / date: _____

Common failures to check yourself against

- Logging enabled but never reviewed — satisfying half the standard and failing the other half
- Read access to ePHI not captured, so inappropriate record lookups are invisible
- No documented review procedure, reviewer or frequency
- Log review evidenced only by a signature with no record of what was examined
- Logs stored only on the originating host, where an attacker can delete them
- Retention set to weeks or months, so investigations and audits have nothing to examine
- Privileged users able to alter or clear logs without trace
- Unsynchronised clocks making cross-system correlation unreliable
- Cloud services, APIs and database tools excluded from logging entirely
- Alert volume so high that alerts are routinely ignored

Beyond the minimum

- Centralise logs into a SIEM or equivalent so correlation across systems is possible
- Automate the detection patterns that matter clinically: same-surname lookups, VIP records, employee self-access, out-of-hours access and bulk export
- Make log review a scheduled, evidenced task with a named owner rather than an aspiration
- Tune alerts deliberately — unreviewable alert volume is functionally the same as no monitoring
- Synchronise time across all systems via NTP so timelines hold up under investigation
- Use append-only or write-once storage for audit data, and restrict access to it
- Retain compliance-relevant logs for six years to align with 164.316(b)(2)
- Report review metrics to leadership so the activity is visible and resourced
- Include cloud services, APIs and database administration tools in log coverage

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.3.2

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