HIPAA AUDITORS

Access Control Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.312(a)(1) — Access Control

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*.

© 2026 HIPAA Auditors. Provided for your internal compliance use. This document is general information, not legal advice, and does not create an auditor–client relationship.

The requirement

Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.

45 CFR 164.312(a)(1) · Technical Safeguards

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

Implementation steps

	Implement technical policies and procedures so that only persons or software programs granted rights under 164.308(a)(4) can reach ePHI. Access control is the standard; four implementation specifications sit beneath it
	Required specifications:
	Unique user identification — 164.312(a)(2)(i). Assign every user a distinct name or number and never permit shared or generic logins. Without unique identity, audit logs cannot attribute activity to a person, and both accountability and the sanction process collapse
	Emergency access procedure — 164.312(a)(2)(ii). Establish a documented route to ePHI when normal authentication is unavailable: a break-glass account, a sealed credential envelope, or a documented escalation to a named administrator. It must be tested, logged and reviewed after every use
	Addressable specifications:
	Automatic logoff — 164.312(a)(2)(iii). Terminate sessions after a defined period of inactivity. Set the interval from the risk of the location: short in shared clinical areas, longer where a workstation is physically controlled
	Encryption and decryption — 164.312(a)(2)(iv). Encrypt ePHI at rest where reasonable and appropriate. Where you decide not to, record the reasoning and the alternative safeguard. Encryption is also the only route to the breach-notification safe harbour at 164.402
	Implementation approach:
	- Build the access model from job function, not from individual request, so entitlements are reviewable
	- Apply least privilege and separation of duties; restrict and separately log administrative rights
	- Provision through a single authoritative process tied to HR joiners, movers and leavers
	- Review entitlements at least quarterly, and immediately on role change or termination
	- Extend the same model to databases, backups, reporting tools and cloud consoles, not just the clinical application

Evidence to produce and retain

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

- [ ] **Access control policy and supporting procedures**
  Location: _____ Owner: _____
- [ ] **Role definitions with the ePHI entitlements attached to each**
  Location: _____ Owner: _____
- [ ] **Unique user identification standard, and any approved exception with justification**
  Location: _____ Owner: _____
- [ ] **Emergency access (break-glass) procedure, test records and post-use review log**
  Location: _____ Owner: _____
- [ ] **Automatic logoff configuration, with the inactivity interval per location and the risk basis for it**
  Location: _____ Owner: _____
- [ ] **Encryption-at-rest decision record, or documented equivalent alternative under 164.306(d)**
  Location: _____ Owner: _____
- [ ] **Access request, approval, modification and revocation records**
  Location: _____ Owner: _____
- [ ] **Periodic entitlement review evidence, including reviewer, date and actions taken**
  Location: _____ Owner: _____
- [ ] **Termination checklists showing access removal, with timestamps**
  Location: _____ Owner: _____
- [ ] **Privileged account inventory and approval records**
  Location: _____ Owner: _____

How this gets tested

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

- [ ] **Reconcile the full user list against current HR records and confirm every account maps to one identified individual**
  Result: _____ Tested by / date: _____
- [ ] **Search for shared, generic, default and service accounts, and confirm each is either removed or justified and controlled**
  Result: _____ Tested by / date: _____
- [ ] **Sample recent leavers and confirm access was revoked, checking the actual timestamp against policy**
  Result: _____ Tested by / date: _____
- [ ]

	Sample recent role changes and confirm entitlements were reduced, not just added to Result: _____ Tested by / date: _____
	Attempt access to ePHI with an account that should not hold it, and confirm denial is enforced and logged Result: _____ Tested by / date: _____
	Execute the emergency access procedure in a controlled test and confirm it works, is logged and triggers review Result: _____ Tested by / date: _____
	Verify automatic logoff by leaving a session idle past the configured interval on each workstation class Result: _____ Tested by / date: _____
	Confirm encryption at rest on servers, laptops, mobile devices, removable media and backups Result: _____ Tested by / date: _____
	Review privileged accounts and confirm administrative rights are separately approved and monitored Result: _____ Tested by / date: _____
	Confirm access controls apply to backup copies, test environments and reporting databases holding real ePHI Result: _____ Tested by / date: _____

Common failures to check yourself against

- Shared or generic logins that make audit trails unattributable
- Terminated employees retaining active accounts, sometimes for months
- Access accumulating across role changes so long-tenured staff hold far more than their job requires
- No emergency access procedure, or one that has never been tested
- Automatic logoff disabled for convenience with no documented risk decision
- Treating the addressable encryption specification as optional and recording no decision at all
- Entitlement reviews that are signed off without anyone actually examining the entitlements
- Access controls applied to the main application but not to backups, test copies or reporting databases
- Unmanaged service and integration accounts holding broad standing access to ePHI

Beyond the minimum

- Enforce role-based access built from job function, and review the role catalogue annually
- Deploy multi-factor authentication for remote access, administrative accounts and any internet-facing system
- Remove standing administrative privilege in favour of just-in-time elevation with automatic expiry
- Keep the leaver process automated from the HR record so revocation cannot depend on someone remembering
- Encrypt ePHI at rest everywhere it is reasonable, and record the decision where it is not
- Alert on privileged account creation, group membership change and failed authorisation spikes
- Test the emergency access procedure at least annually, and treat every real use as a reviewable event

- Include cloud consoles, database admin tools and integration accounts in the same access model
- Attest entitlements with the business owner who understands the job, not only with IT

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.3.1

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