HIPAA AUDITORS

Workstation Use Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.310(b) — Workstation Use

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 policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

45 CFR 164.310(b) · Physical Safeguards

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

Implementation steps

- [ ] **Develop comprehensive workstation use policies including:**
- [ ] **Workstation use policies and procedures**
- [ ] **Physical security requirements for workstations**
- [ ] **Workstation configuration standards**
- [ ] **User responsibilities for workstation security**
- [ ] **Workstation monitoring and auditing procedures**
- [ ] **Workstation disposal and sanitization procedures**
- [ ] **Key components:**
- [ ] **- Workstation use policies**
- [ ] **- Physical security requirements**
- [ ] **- Configuration standards**
- [ ] **- User responsibilities**
- [ ] **- Monitoring and auditing**
- [ ] **- Disposal procedures**

Evidence to produce and retain

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

- [ ] **Workstation use policies and procedures**
  Location: _____ Owner: _____
- [ ] **Physical security requirements**
  Location: _____ Owner: _____
- [ ]

	Location: _____ Owner: _____
	Workstation configuration standards Location: _____ Owner: _____
	Monitoring and auditing procedures Location: _____ Owner: _____
	Disposal and sanitization procedures Location: _____ Owner: _____
	Training materials and records Location: _____ Owner: _____

How this gets tested

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

	Review workstation use policies Result: _____ Tested by / date: _____
	Test physical security controls Result: _____ Tested by / date: _____
	Verify configuration standards Result: _____ Tested by / date: _____
	Review user training records Result: _____ Tested by / date: _____
	Test monitoring and auditing capabilities Result: _____ Tested by / date: _____
	Verify disposal procedures Result: _____ Tested by / date: _____
	Review policy compliance Result: _____ Tested by / date: _____

Common failures to check yourself against

- Lack of workstation use policies
- Inadequate physical security for workstations
- Insufficient workstation configuration standards
- Poor user training on workstation security
- Inadequate monitoring of workstation use
- Insufficient disposal procedures

Beyond the minimum

- Develop comprehensive workstation policies
- Implement physical security controls
- Establish configuration standards
- Provide user training and awareness
- Monitor workstation use regularly
- Implement proper disposal procedures
- Regular review and update of policies

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.2.2 NIST Cybersecurity Framework: PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7 NIST SP 800-53: PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-7, PE-8, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, PE-17, PE-18, PE-19, PE-20, PE-21, PE-22, PE-23, PE-24, PE-25

Sign-off

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