HIPAA AUDITORS

# Workstation Security Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.310(c) — Workstation Security

| | |
|---|---|
| **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 physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

*45 CFR 164.310(c) · Physical Safeguards*

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

## Implementation steps

- [ ] **Implement comprehensive workstation controls including:**
- [ ] **Physical access controls for workstations**
- [ ] **User authentication and authorization**
- [ ] **Workstation configuration management**
- [ ] **Monitoring and logging of workstation access**
- [ ] **Workstation security policies and procedures**
- [ ] **Regular security assessments of workstations**
- [ ] **Key components:**
- [ ] **- Physical access restrictions**
- [ ] **- User authentication requirements**
- [ ] **- Configuration management**
- [ ] **- Monitoring and logging**
- [ ] **- Security policies**
- [ ] **- Regular assessments**

## Evidence to produce and retain

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

- [ ] **Workstation control policies and procedures**
  Location: _____ Owner: _____
- [ ] **Physical access control documentation**
  Location: _____ Owner: _____
- [ ] **User authentication procedures**
  Location: _____ Owner: _____

- [ ] **Configuration management procedures**
  Location: _____ Owner: _____
- [ ] **Monitoring and logging procedures**
  Location: _____ Owner: _____
- [ ] **Security assessment 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 control policies**
  Result: _____ Tested by / date: _____
- [ ] **Test physical access controls**
  Result: _____ Tested by / date: _____
- [ ] **Verify user authentication**
  Result: _____ Tested by / date: _____
- [ ] **Review configuration management**
  Result: _____ Tested by / date: _____
- [ ] **Test monitoring and logging**
  Result: _____ Tested by / date: _____
- [ ] **Verify security policies**
  Result: _____ Tested by / date: _____
- [ ] **Conduct security assessments**
  Result: _____ Tested by / date: _____

## Common failures to check yourself against

- Inadequate physical access controls
- Insufficient user authentication
- Poor configuration management
- Inadequate monitoring and logging
- Insufficient security policies
- Lack of regular security assessments

## Beyond the minimum

- Implement strong physical access controls
- Use multi-factor authentication

- Establish configuration management
- Monitor and log all access
- Develop comprehensive security policies
- Conduct regular security assessments
- Regular training and awareness

*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** |
| | | |