| OpsAuditHub<br>opsauditihub.com | DOC ID: **SAF-0157** | REVISION: **Rev 2.4 (2026)** |
|---|---|---|
| | STANDARD: **HIPAA Privacy Rule 45 CFR Part 160 and Subparts A and E of Part 164** | AUDIT FREQUENCY: **Quarterly Audit** |

# Hipaa Privacy Compliance Audit Compliance Checklist

**Operational Scope:** This audit checklist establishes a standardized protocol for evaluating administrative, physical, and technical safeguards across healthcare facilities. Its primary objective is to mitigate unauthorized Protected Health Information (PHI) exposure and ensure mandatory compliance with federal privacy standards.

| | |
|---|---|
| **MANDATORY PPE:** | Facility Security Badges, Privacy Filter Glasses (for mobile workstation testing), Confidential Shred Bin Access Keys, Nitrile Gloves (for handling secure media) |
| **PREREQUISITES:** | Notify clinic administration and IT privacy officer of active audit initiation. \| Review previous quarterly HIPAA audit corrective action logs. \| Ensure master key access to all medical records storage areas and server rooms. |

## ADMINISTRATIVE AND PERSONNEL SAFEGUARDS

| # | COMPONENT / ITEM | VERIFICATION CRITERIA & ACCEPTANCE STANDARD | SEVERITY | STATUS |
|---|---|---|---|---|
| 1 | **Workforce Privacy Training Records** | All active employees, contractors, and volunteers have completed initial HIPAA privacy training within 30 days of hire and documented annual refreshers. | **Critical (Immediate Out of Service)** | **[ ] PASS [ ] FAIL [ ] N/A** |
| 2 | **Notice of Privacy Practices (NPP)** | Current NPP is visibly posted in public reception areas, readily available upon request, and accessible on the clinic website. | **Warning** | **[ ] PASS [ ] FAIL [ ] N/A** |
| 3 | **Business Associate Agreements (BAAs)** | Active, signed BAAs are on file for all third-party vendors, software providers, and billing services handling PHI. | **Critical (Immediate Out of Service)** | **[ ] PASS [ ] FAIL [ ] N/A** |
| 4 | **Sanction Policy Enforcement** | Documentation exists showing consistent enforcement of disciplinary sanctions against workforce members who violate privacy policies. | **Warning** | **[ ] PASS [ ] FAIL [ ] N/A** |

## PHYSICAL AND FACILITY SAFEGUARDS

| # | COMPONENT / ITEM | VERIFICATION CRITERIA & ACCEPTANCE STANDARD | SEVERITY | STATUS |
|---|---|---|---|---|
| 5 | **Reception and Check-in Areas** | Acoustic and visual barriers prevent patients from overhearing verbal PHI or viewing sign-in sheets containing sensitive medical data. | **Critical (Immediate Out of Service)** | **[ ] PASS [ ] FAIL [ ] N/A** |
| 6 | **Workstation Positioning** | Computer monitors displaying EHR or scheduling software are angled away from public view or equipped with functional privacy screens. | **Warning** | **[ ] PASS [ ] FAIL [ ] N/A** |
| 7 | **Physical Records Storage Security** | Paper charts, physical archives, and medical storage rooms remain locked when unattended; keys are restricted to authorized personnel only. | **Critical (Immediate Out of Service)** | **[ ] PASS [ ] FAIL [ ] N/A** |
| 8 | **Secure Disposal Receptacles** | Dedicated locked shredding bins for PHI waste are securely anchored, uncompromised, and not overflowing. | **Critical (Immediate Out of Service)** | **[ ] PASS [ ] FAIL [ ] N/A** |

## TECHNICAL AND ACCESS CONTROL SAFEGUARDS

| # | COMPONENT / ITEM | VERIFICATION CRITERIA & ACCEPTANCE STANDARD | SEVERITY | STATUS |
|---|---|---|---|---|
| 9 | **Unique User Identification** | Generic or shared login accounts are strictly prohibited; every staff member accesses systems via unique individual credentials. | **Critical (Immediate Out of Service)** | **[ ] PASS [ ] FAIL [ ] N/A** |
| 10 | **Automatic Logoff Mechanisms** | EHR and clinical workstations engage automatic screen locking or logoff sequences after a period of inactivity not exceeding 10 minutes. | **Warning** | **[ ] PASS [ ] FAIL [ ] N/A** |
| 11 | **Transmission Security and Encryption** | All external electronic communications containing PHI, including emails and file transfers, utilize validated end-to-end encryption. | **Critical (Immediate Out of Service)** | **[ ] PASS [ ] FAIL [ ] N/A** |

| | | |
|---|---|---|
| **Certified Privacy Compliance Auditor / OpsAuditHub Inspector Signature:** _____ | **Date / Time:** _____ | **Badge / Cert #:** _____ |
| **Chief Compliance Officer / Clinic Operations Manager Sign-off:** _____ | **Review Date:** _____ | **Audit Status:** [ ] Approved [ ] Rectify |

**COMPLIANCE NOTICE:** This document must be archived for a minimum of 6 years in accordance with HIPAA administrative simplification recordkeeping guidelines (45 CFR § 164.530).

**DIGITAL INSPECTION UPGRADE:** Run this audit on mobile/tablet, attach photos & automate compliance records. **Start Free Mobile Audit →**