ANATOMYIT

Healthcare

TRUSTED. STRATEGIC. SECURE.

The 2026 HIPAA Compliance Checklist

Essential Requirements Every Healthcare Organization Must Meet

✓ Updated February 2026

✓ Includes New Security Rule Requirements

✓ Based on Official HHS & NIST Guidance

Call 888-816-9272

Visit anatomyit.com

HIPAA violations cost healthcare organizations $50,000+ per incident. Use this checklist to ensure your practice stays compliant and protects patient data.

HOW TO USE THIS CHECKLIST

✓ Print or save digitally for ongoing reference
✓ Check off items as you complete them - this is a working document
✓ Prioritize ⚠ CRITICAL items - especially proposed 2026 requirements
✓ Address 🛑 HIGH PRIORITY items - these are common violation areas
✓ Document everything - HIPAA compliance requires proof, not just completion
✓ Review quarterly - HIPAA is not "one and done," it requires ongoing maintenance
✓ Keep for 6+ years - retention requirements apply to your compliance documentation
✓ Update when rules change - monitor www.hhs.gov/hipaa for updates to regulations

⚠ **CRITICAL** - New 2026 requirement or proposed change

🛑 **HIGH PRIORITY** - Common violation, OCR enforcement focus

🟨 **MEDIUM** - Addressable / required implementation

🔺 **FOUNDATIONAL** - Basic requirement, essential compliance

SECTION 1: ADMINISTRATIVE SAFEGUARDS

From HHS Security Rule 45 CFR § 164.308 + NIST SP 800-66r2, Section 5.1 (§§ 5.1.1–5.1.9)

Administrative safeguards are policies and procedures designed to manage the selection, development, and implementation of security measures.

- [ ] **Appoint a HIPAA Privacy Officer and Security Officer**
  Required: Designated responsible parties for HIPAA compliance oversight
  Reference: 45 CFR § 164.530(a)(1) | 45 CFR § 164.308(a)(2)

- [ ] **Conduct annual HIPAA risk analysis**
  Identify where PHI/ePHI is created, received, stored, transmitted; assess threats and vulnerabilities
  Reference: 45 CFR § 164.308(a)(1)(ii)(A)

- [ ] **Implement workforce security procedures**
  Authorization/supervision of workforce members who access ePHI; procedures for granting, modifying, and terminating access | Reference: 45 CFR § 164.308(a)(3)

- [ ] **Provide HIPAA training to all workforce members**
  Initial training for new hires + refresher training when policies change materially
  Reference: 45 CFR § 164.530(b)(1) | 45 CFR § 164.308(a)(5)

- [ ] **Establish written policies and procedures**
  Document how you comply with each HIPAA Privacy and Security Rule requirement
  Reference: 45 CFR § 164.316(a) | 45 CFR § 164.530(i)

- [ ] **Create and test incident response plan**
  Procedures for responding to security incidents and breaches; document incidents and outcomes
  Reference: 45 CFR § 164.308(a)(6)

- [ ] **Maintain Business Associate Agreements (BAAs)**
  Signed agreements with all vendors who access PHI (EHR vendors, IT providers, cloud services, billing companies, shredding services) | Reference: 45 CFR § 164.308(b) | 45 CFR § 164.504(e)

- [ ] **Implement access controls and user authentication**
  Unique user IDs (required), role-based access, authorization procedures; MFA strongly recommended
  Reference: 45 CFR § 164.308(a)(4) | 45 CFR § 164.312(a)(1)

- [ ] **Review and audit system activity logs regularly**
  Monitor who accessed what PHI and when; review frequency based on risk assessment
  Reference: 45 CFR § 164.308(a)(1)(ii)(D) | 45 CFR § 164.312(b)

- [ ] **Document HIPAA compliance efforts**
  Retain all policies, risk assessments, training records, incident reports, and audit logs for 6+ years
  Reference: 45 CFR § 164.316(b)(2) | 45 CFR § 164.530(j)

SECTION 2: PHYSICAL SAFEGUARDS

From HHS Security Rule 45 CFR § 164.310 + NIST SP 800-66r2, Section 5.2 (§§ 5.2.1–5.2.4)

Physical safeguards are physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.

- [ ] **Control facility access to systems with ePHI**
  Locked server rooms, badge access, visitor logs, security cameras, controlled access to areas with ePHI
  Reference: 45 CFR § 164.310(a)(1)

- [ ] **Implement workstation security controls**
  Privacy screens, auto-lock after inactivity, workstation positioning away from public view
  Reference: 45 CFR § 164.310(c)

- [ ] **Secure mobile devices and laptops**
  Encryption required, remote wipe capability, Mobile Device Management (MDM) for devices with ePHI
  Reference: 45 CFR § 164.310(d)(1)

- [ ] **Dispose of PHI securely**
  Shred paper records, wipe/destroy hard drives before disposal, degauss magnetic media
  Reference: 45 CFR § 164.310(d)(2)

- [ ] **Maintain device and media inventory**
  Track all hardware containing ePHI (computers, servers, backup drives, tablets, USB drives, digital copiers)
  Reference: 45 CFR § 164.310(d)(1)

- [ ] **Implement physical disaster recovery**
  Off-site backups, tested recovery procedures, emergency access protocols for facility access
  Reference: 45 CFR § 164.310(a)(2)(i)

- [ ] **Secure digital copiers and printers**
  Erase hard drives before disposal/return, require authentication to print/copy, secure print release
  Reference: 45 CFR § 164.310(d)(2)

SECTION 3: TECHNICAL SAFEGUARDS

From HHS Security Rule 45 CFR § 164.312 + NIST SP 800-66r2, Section 5.3 (§§ 5.3.1–5.3.5)

Technical safeguards are the technology and the policy and procedures for its use that protect ePHI and control access to it.

- [ ] **Encrypt ePHI at rest and in transit**
  CURRENT: Addressable specification - implement or document why not appropriate PROPOSED 2026: May become required (pending Security Rule finalization) Best practice: **AES-256** for stored data, TLS 1.2+ for transmission | Reference: 45 CFR § 164.312(a)(2)(iv) | 45 CFR § 164.312(e)(2)(ii)

- [ ] **Implement multi-factor authentication (MFA)**
  CURRENT: Not explicitly required, but strongly recommended PROPOSED 2026: Expected to be mandatory for all ePHI access Implement now as best practice; "vendor doesn't support" will not be valid excuse Reference: Proposed NPRM (December 27, 2024), finalization expected May 2026

- [ ] **Deploy automatic log-off after inactivity**
  Sessions timeout after predetermined time (15 minutes typical for high-risk areas)
  Reference: 45 CFR § 164.312(a)(2)(iii) - Addressable

- [ ] **Install and maintain firewall protection**
  Network segmentation, intrusion detection/prevention systems, GeoIP filtering, firmware updates, boundary protection | Reference: 45 CFR § 164.312(a) - Access Control (technical policies)

- [ ] **Implement Endpoint Detection & Response (EDR)/anti-malware software**
  Automatic updates, real-time scanning, regular full system scans, protection from malicious software
  Reference: 45 CFR § 164.308(a)(5)(ii)(B)

- [ ] **Conduct regular software patching and updates**
  OS, applications, security software updated within 30 days of critical patch release; prioritize based on risk
  Reference: 45 CFR § 164.308(a)(1) - Risk Management

- [ ] **Perform regular data backups**
  3-2-1 rule recommended: 3 copies, 2 different media types, 1 offsite PROPOSED 2026: Testable recovery required; test restoration quarterly | Reference: 45 CFR § 164.308(a)(7)(ii)(A) - Data Backup Plan

- [ ] **Deploy email security controls**
  Encrypted email for ePHI transmission, anti-phishing training, anti-spam filtering, secure file sharing alternatives | Reference: 45 CFR § 164.312(e)(1) - Transmission Security

- [ ] **Implement network monitoring and intrusion detection**
  24/7 monitoring where appropriate, alerts for suspicious activity, security event logging and review
  Reference: 45 CFR § 164.308(a)(1)(ii)(D) | 45 CFR § 164.312(b)

SECTION 4: BREACH NOTIFICATION REQUIREMENTS

From HHS Breach Notification Rule 45 CFR §§ 164.400–414

The Breach Notification Rule requires covered entities and business associates to provide notification following a breach of unsecured protected health information.

- [ ] **Understand what constitutes a breach**
  Unauthorized acquisition, access, use, or disclosure of PHI that compromises security or privacy of the information | Reference: 45 CFR § 164.402

- [ ] **Conduct breach risk assessment immediately**
  If incident occurs: Was PHI encrypted? What information was exposed? What is the likelihood of further use or disclosure? | Reference: 45 CFR § 164.402(2)

- [ ] **Notify affected individuals within 60 days**
  Written notice including: what happened, what information was involved, what you're doing to investigate and mitigate, what individuals should do to protect themselves | Reference: 45 CFR § 164.404(b)

- [ ] **Report breaches of 500+ individuals to HHS immediately**
  Submit within 60 days of discovery via HHS Breach Portal; notify prominent media outlets in affected geographic areas | Reference: 45 CFR § 164.404(c) | 45 CFR § 164.406

- [ ] **Report breaches of <500 individuals annually**
  Submit log to HHS within 60 days after end of calendar year; maintain internal breach log
  eference: 45 CFR § 164.404(c)

SECTION 5: PRIVACY RULE COMPLIANCE

HHS Privacy Rule 45 CFR §§ 164.500–534 + Feb 2026 NPP Update (45 CFR § 164.520)

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other individually identifiable health information.

- [ ] ⚠ **Provide Notice of Privacy Practices (NPP) to patients**
  UPDATE REQUIRED BY FEBRUARY 16, 2026 per April 2024 Final Rule Explain how PHI is used/disclosed, patient rights, complaint procedures; obtain acknowledgment of receipt | Reference: 45 CFR § 164.520

- [ ] 🛑 **Honor patient rights to access PHI**
  Provide copies of records within 30 days of request (may extend once for 30 days with written notice and reason) | Reference: 45 CFR § 164.524

- [ ] 🟨 **Allow patients to request amendments to PHI**
  Establish process for requesting changes to records; must respond within 60 days; may deny under specific circumstances | Reference: 45 CFR § 164.526

- [ ] 🟨 **Provide accounting of disclosures when requested**
  Track and report PHI disclosures for past 6 years (exceptions: treatment, payment, operations, patient-authorized) | Reference: 45 CFR § 164.528

- [ ] 🟨 **Obtain patient authorization for non-standard uses**
  Written, signed consent required for marketing, research, sale of PHI, psychotherapy notes, and other non-routine uses | Reference: 45 CFR § 164.508

- [ ] 🛑 **Implement minimum necessary standard**
  Limit PHI access and disclosure to minimum amount reasonably necessary to accomplish intended purpose Reference: 45 CFR § 164.502(b) | 45 CFR § 164.514(d)

SECTION 6: 2026-SPECIFIC UPDATES

From HHS Proposed Security Rule NPRM (December 27, 2024) + HHS

These requirements are based on Proposed Rulemaking published December 27, 2024. Final rules expected May 2026 with implementation deadlines to be determined. Monitor www.hhs.gov/hipaa for updates.

- [ ] ⚠ **Create and maintain network mapping**
  PROPOSED 2026 (Not yet finalized) Document ePHI data flows through your network; update annually or after significant environmental/operational changes | Reference: Proposed 45 CFR § 164.316(b)(2)(iii)

- [ ] ⚠ **Obtain annual vendor compliance attestations**
  PROPOSED 2026 (Not yet finalized) Written verification that Business Associates have implemented required technical safeguards; BAA alone insufficient | Reference: Proposed Security Rule Updates (December 2024 NPRM)

- [ ] ⚠ **Eliminate "addressable" safeguard exemptions**
  PROPOSED 2026 (Not yet finalized) Nearly all implementation specifications to become mandatory with limited exceptions; document full compliance | Reference: Proposed Security Rule Overhaul (December 2024 NPRM)

- [ ] ⚠ **Prepare for annual compliance audits**
  PROPOSED 2026 (Not yet finalized) Business Associates must conduct formal compliance audits and share results with covered entity clients; comprehensive documentation required | Reference: Proposed Security Rule Updates (December 2024 NPRM)

- [ ] ⚠ **Implement 24-hour breach reporting (Business Associates)**
  PROPOSED 2026 (Not yet finalized) CURRENT: 60 days per 45 CFR § 164.410 PROPOSED: Business Associates must notify covered entities within 24 hours of breach discovery
  Reference: Proposed NPRM (December 2024)

Most Common HIPAA Violations

Based on HHS Office for Civil Rights Breach Portal Data (January - September 2025)

1. **Failure to conduct risk assessments** - 43% of violations
2. **Lack of Business Associate Agreements** - 31% of violations
3. **Insufficient access controls** - 28% of violations
4. **No encryption of ePHI** - 24% of violations
5. **Inadequate workforce training** - 22% of violations

Source: HHS OCR Breach Portal Analysis

Additional Resources

- HHS HIPAA Homepage - www.hhs.gov/hipaa
- OCR Security Risk Assessment Tool - www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
- NIST Cybersecurity Framework - www.nist.gov/cyberframework
- NIST Special Publication 800-66 Rev. 2 "Implementing the HIPAA Security Rule: A Cybersecurity Resource Guide" - csrc.nist.gov/pubs/sp/800/66/r2/final
- HIPAA Journal (Industry News & Guidance) - www.hipaajournal.com
- OCR Cybersecurity Newsletters - www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter

DISCLAIMER

This checklist is based on HIPAA Security Rule (45 CFR §§ 164.302-318), Privacy Rule (45 CFR §§ 164.500-534), and NIST SP 800-66 Rev. 2. Updated February 2026. This document is for informational purposes only and does not constitute legal advice. Consult with qualified HIPAA compliance professionals for specific guidance.

Want to achieve compliance?

This checklist covers 45+ critical HIPAA requirements across all major rule categories. Use it as your roadmap to compliance, but remember: HIPAA compliance is an ongoing process, not a one-time project.

Contact us at anatomyit.com/lets-connect/