HIPAA COMPLIANCE CHECKLIST

HIPAA compliance is predictable. Because the requirements haven't changed dramatically in years, you can work through them systematically.

This checklist breaks HIPAA into five sections. Work through each one, check off what you have, and flag what you're missing. By the end, you'll know exactly where your practice stands and what to fix first.

Last Updated:_____ Updated By:_____

PRIVACY RULE COMPLIANCE CHECKLIST

The Privacy Rule controls how you use and share protected health information (PHI). It's about policies, patient rights, and who can access what.

BUSINESS ASSOCIATE AGREEMENTS

Without exception, every vendor that touches PHI needs a signed Business Associate Agreement (BAA).

- ❒ IT provider has signed BAA on file
- ❒ Billing company has signed BAA on file
- ❒ EHR/EMR vendor has signed BAA on file
- ❒ Transcription service has signed BAA on file
- ❒ Answering service has signed BAA on file
- ❒ Shredding company has signed BAA on file
- ❒ Cloud storage providers (Dropbox, Google Drive, etc.) have signed BAAs
- ❒ All BAAs have been reviewed in the past 12 months
- ❒ BAAs include breach notification requirements

PATIENT RIGHTS DOCUMENTATION

Your practice needs documentation for each of the following patient rights required under HIPAA:

- ❒ Notice of Privacy Practices posted in waiting area
- ❒ Notice of Privacy Practices available on website
- ❒ Written process for patients to request their records
- ❒ Records provided within 30 days of request (Missouri standard)
- ❒ Written process for patients to request amendments to records
- ❒ Written process for accounting of disclosures
- ❒ Authorization forms available for non-standard disclosures

ACCESS CONTROLS

Not everyone in your practice needs access to everything.

- ❒ Role-based access defined (front desk vs. clinical vs. billing)
- ❒ EHR access levels match job responsibilities
- ❒ Terminated employee access revoked within 24 hours
- ❒ Shared login accounts eliminated (each user has unique credentials)
- ❒ Access logs reviewed quarterly for unusual activity

KEY CONTACTS

The Security Rule focuses on electronic PHI (ePHI).

TECHNICAL SAFEGUARDS

- ❒ All ePHI encrypted at rest (on servers, workstations, laptops)
- ❒ All ePHI encrypted in transit (email, file transfers, remote access)
- ❒ Automatic logoff enabled on all workstations (15 minutes or less)
- ❒ Unique user IDs for every employee
- ❒ Strong password policy enforced (12+ characters, complexity requirements)
- ❒ Multi-factor authentication (MFA) enabled for EHR access
- ❒ MFA enabled for email access
- ❒ MFA enabled for remote access/VPN
- ❒ Antivirus/endpoint protection on all devices
- ❒ Firewall configured and monitored
- ❒ Audit logs enabled for ePHI access

BACKUP AND RECOVERY

- ❒ Daily backups of all ePHI systems
- ❒ Backups stored offsite or in HIPAA-compliant cloud
- ❒ Backup encryption verified
- ❒ Backup restoration tested quarterly
- ❒ Recovery time objective (RTO) documented
- ❒ Recovery point objective (RPO) documented

PHYSICAL SECURITY

Physical access matters as much as digital access.

- ❒ Server room locked with restricted key/badge access
- ❒ Workstations positioned to prevent screen visibility from public areas
- ❒ Paper PHI secured in locked cabinets after hours
- ❒ Visitor sign-in required for non-patient visitors
- ❒ Security cameras covering entry points (with appropriate retention policies)
- ❒ Mobile devices (laptops, tablets) encrypted and password-protected
- ❒ Mobile device remote wipe capability enabled

BREACH NOTIFICATION READINESS CHECKLIST

HHS requires notification within 60 days of discovering a breach.

INCIDENT RESPONSE PLAN

- ❒ Written incident response plan exists
- ❒ Plan reviewed and updated annually
- ❒ Incident response team identified (who does what)
- ❒ Contact information current for response team members
- ❒ After-hours contact procedures documented
- ❒ IT provider's breach response SLA documented

NOTIFICATION PROCEDURES

- ❒ Patient notification letter template prepared
- ❒ HHS notification process documented (breaches of 500+ individuals)
- ❒ Media notification process documented (breaches of 500+ in single state/jurisdiction)
- ❒ Missouri Attorney General notification requirements documented
- ❒ Documentation retention process for breach investigations (6 years minimum)

DETECTION CAPABILITIES

- ❒ Network monitoring for unusual data transfers
- ❒ Failed login attempt alerts configured
- ❒ After-hours access alerts configured
- ❒ Email security monitoring (phishing attempts, compromised accounts)
- ❒ Endpoint detection and response (EDR) deployed

ADMINISTRATIVE SAFEGUARDS CHECKLIST

Administrative safeguards are the policies, procedures, and people that hold everything together.

RISK ASSESSMENT

HHS specifically requires a formal risk assessment.

- ❒ Formal risk assessment completed
- ❒ Risk assessment conducted within past 12 months
- ❒ Risk assessment covers all ePHI systems
- ❒ Identified risks documented with severity ratings
- ❒ Remediation plan created for high-priority risks
- ❒ Remediation progress tracked and documented

POLICIES AND PROCEDURES:

- ❒ Written HIPAA policies exist and are accessible to staff
- ❒ Policies cover Privacy Rule requirements
- ❒ Policies cover Security Rule requirements
- ❒ Policies cover Breach Notification requirements
- ❒ Policies reviewed and updated annually
- ❒ Policy changes communicated to all staff
- ❒ Policy acknowledgment signed by all employees

DESIGNATED ROLES

HIPAA requires specific people to own compliance.

- ❒ Privacy Officer designated (by name, not just title)
- ❒ Security Officer designated (can be same person in small practices)
- ❒ Backup contacts identified if primary officers are unavailable
- ❒ Officers have completed HIPAA training specific to their role

WORKFORCE TRAINING

- ❒ All employees complete HIPAA training at hire
- ❒ Annual HIPAA refresher training conducted
- ❒ Training completion documented and retained
- ❒ Training covers phishing awareness and social engineering
- ❒ Training covers physical security (tailgating, visitor management)
- ❒ Training includes practice-specific scenarios
- ❒ Sanctions policy documented for HIPAA violations

ONGOING COMPLIANCE CHECKLIST

Compliance isn't a one-time project. These items keep you current.

ANNUAL REVIEWS

- ❒ Risk assessment scheduled annually
- ❒ BAA inventory reviewed annually
- ❒ Policies reviewed and updated annually
- ❒ Training conducted annually
- ❒ Business continuity plan tested annually
- ❒ Access permissions audited annually

STAYING CURRENT

- ❒ HHS guidance monitored for updates (hhs.gov/hipaa)
- ❒ Missouri-specific requirements tracked
- ❒ IT provider provides quarterly security reports
- ❒ Compliance status reviewed in staff meetings quarterly

DOCUMENTATION RETENTION

- ❒ HIPAA-related documents retained for 6 years minimum
- ❒ Training records retained for 6 years minimum
- ❒ Incident reports retained for 6 years minimum
- ❒ BAAs retained for 6 years after relationship ends

This template provides a starting framework for HIPAA compliance. For comprehensive support and planning assistance tailored to your practice, consult with qualified IT professionals.

Prepared by: NOC Technology
Download the latest version at: noctechnology.com

24/7 Emergency Support: 636.390.6621

© 2025 NOC Technology. This checklist is free to use and distribute.
We only ask that you keep the attribution intact.

ABOUT NOC TECHNOLOGY

Our comprehensive approach combines advanced technology with human expertise to create a solid defensive posture.

Established in 2009, NOC Technology is a leading managed support provider (MSP) providing quality IT support for St. Louis, MO and beyond. We serve as an extension of our client's staff, providing 24x7 security monitoring and unlimited remote support with direct access to our IT experts.

info@noctechs.com
noctechnology.com