HIPAA Compliance Checklist: Complete Guide for Healthcare Organizations

Last Updated: September 2025

Compliance Standard: HIPAA/HITECH Act

Applicable To: Covered Entities & Business Associates

This comprehensive checklist covers all 54 HIPAA implementation specifications across the Privacy, Security, and Breach Notification Rules.

Part 1: Foundational Requirements

Determine Your HIPAA Status

☐ **Identify if you are a Covered Entity**

- Healthcare providers who transmit health information electronically
- Health plans (insurance companies, HMOs, Medicare, Medicaid)
- Healthcare clearinghouses

☐ **Identify if you are a Business Associate**

- Perform functions involving PHI on behalf of a Covered Entity
- Examples: billing services, cloud storage, IT support, legal services

☐ **Document your HIPAA classification and scope**

Business Associate Management

□ **Create inventory of all Business Associates**

□ **Execute Business Associate Agreements (BAAs) with ALL vendors who handle PHI**

- Include required provisions for safeguarding PHI
- Specify permitted uses and disclosures
- Include breach notification requirements
- Set termination conditions

□ **Review BAAs annually**

□ **Maintain copies of all BAAs for 6+ years**

Designate Required Officers

□ **Appoint HIPAA Privacy Officer**

- Document appointment in writing
- Define roles and responsibilities
- Provide necessary authority and resources

□ **Appoint HIPAA Security Officer**

- May be same person as Privacy Officer in smaller organizations
- Document appointment and responsibilities
- Ensure appropriate technical expertise

Part 2: Privacy Rule Requirements

Notice of Privacy Practices (NPP)

□ **Develop comprehensive NPP that includes:**

- How PHI may be used and disclosed
- Patient rights regarding their PHI
- Your legal duties regarding PHI
- How to file complaints

□ **Distribute NPP to all patients**

- At first service delivery
- Upon request
- When NPP is revised

□ **Post NPP prominently**

(physical location and website)

□ **Obtain written acknowledgment of receipt**

Patient Rights Management

□ Right to Access

- Establish process for patients to request their records
- Respond within 30 days (one 30-day extension allowed)
- Provide in requested format when possible
- Document all requests and responses

□ Right to Amendment

- Create process for amendment requests
- Respond within 60 days
- Document denials with reasons

□ Right to Accounting of Disclosures

- Track all non-routine disclosures
- Provide accounting within 60 days of request
- Cover 6-year period (excluding TPO disclosures)

□ Right to Restriction

- Process for requesting restrictions on use/disclosure
- Document approved restrictions
- Implement technical controls for restrictions

Minimum Necessary Standard

□ Implement role-based access controls

□ Define minimum necessary for each job role

□ Document access level justifications

□ Review and update quarterly

□ Train workforce on minimum necessary principle

Part 3: Security Rule - Administrative Safeguards

Security Management Process REQUIRED

□ Conduct comprehensive Security Risk Analysis

- Identify all systems that create, receive, maintain, or transmit ePHI
- Document all potential threats and vulnerabilities
- Assess current security measures
- Calculate risk levels (likelihood × impact)
- Prioritize risks for remediation

□ Implement Risk Management Plan

- Address high-priority risks first
- Document mitigation strategies
- Set implementation timelines
- Assign responsible parties

□ Implement Sanction Policy

- Define violations and consequences
- Apply consistently to all workforce members
- Document all sanctions applied

□ Information System Activity Review

- Regular review of audit logs
- Investigate anomalies
- Document review activities

Workforce Security

□ Authorization and/or Supervision

ADDRESSABLE

- Define authorization procedures
- Document supervision requirements
- Implement for workforce and volunteers

□ Workforce Clearance Procedure

ADDRESSABLE

- Background checks where appropriate
- Verification of credentials
- Documentation of clearance

□ Termination Procedures

ADDRESSABLE

- Immediate access revocation upon termination
- Return of all devices and materials
- Remove from all systems
- Change shared passwords

Security Awareness and Training REQUIRED

□ Security Reminders

ADDRESSABLE

- Regular security tips and updates
- Posters, emails, meetings

□ Protection from Malicious Software

ADDRESSABLE

- Anti-malware training
- Phishing awareness
- Safe browsing practices

□ Log-in Monitoring

ADDRESSABLE

- Failed login attempt procedures
- Suspicious activity reporting

□ Password Management

ADDRESSABLE

- Password creation guidelines
- Password protection training
- Multi-factor authentication where appropriate

Contingency Plan REQUIRED

□ Data Backup Plan

REQUIRED

- Define backup frequency
- Test restore procedures
- Offsite storage
- Encryption of backups

□ Disaster Recovery Plan

REQUIRED

- Identify critical systems
- Recovery time objectives
- Alternative processing sites
- Communication procedures

□ Emergency Mode Operation Plan

REQUIRED

- Procedures during emergencies
- Manual processes when systems unavailable
- Security during emergency mode

Part 4: Security Rule - Physical Safeguards

Facility Access Controls REQUIRED

□ Contingency Operations

ADDRESSABLE

- Emergency access procedures
- Alternative sites identified
- Security during emergencies

□ Facility Security Plan

ADDRESSABLE

- Locks, badges, alarms
- Visitor management
- Security personnel

□ Access Control and Validation Procedures

ADDRESSABLE

- Role-based facility access
- Visitor logs
- Escort requirements

□ Maintenance Records

ADDRESSABLE

- Document repairs and modifications
- Verify personnel credentials
- Supervise maintenance activities

Workstation Use REQUIRED

□ **Define proper workstation use policies**

□ **Specify workstation locations**

□ **Screen positioning to prevent unauthorized viewing**

□ **Automatic screen locks**

□ **Clear desk policy**

Device and Media Controls REQUIRED

□ **Disposal**

REQUIRED

- Shredding for paper records
- NIST-compliant data wiping for electronic media
- Certificate of destruction
- Document disposal activities

□ **Media Re-use**

REQUIRED

- Complete data removal before re-use
- Verification procedures
- Documentation

□ **Accountability**

ADDRESSABLE

- Hardware/media inventory
- Tracking system
- Responsible person designation

Part 5: Security Rule - Technical Safeguards

Access Control REQUIRED

□ Unique User Identification

REQUIRED

- Individual user accounts (no sharing)
- Disable generic/default accounts
- Regular account audits

□ Automatic Logoff

ADDRESSABLE

- Set timeout periods
- Force re-authentication
- Configure based on risk

□ Encryption and Decryption

ADDRESSABLE

- Encrypt ePHI at rest
- Document encryption methods
- Key management procedures

□ Emergency Access Procedure

REQUIRED

- Break-glass procedures
- Documentation requirements
- Audit emergency access

Audit Controls REQUIRED

□ **Implement audit logging for all ePHI systems**

□ **Log user activity, access attempts, modifications**

□ **Regular log reviews**

□ **Secure log storage (tamper-proof)**

□ **Retention per state/federal requirements**

Transmission Security REQUIRED

□ **Integrity Controls**

ADDRESSABLE

- Ensure data not improperly modified
- Message authentication codes
- Digital certificates

□ **Encryption**

ADDRESSABLE

- Encrypt ePHI in transit
- VPN for remote access
- Secure email solutions
- HTTPS for web applications

Part 6: Breach Notification Rule

Breach Response Planning

□ Develop Breach Response Plan including:

- Discovery and reporting procedures
- Investigation team and roles
- Forensic analysis procedures
- Risk assessment methodology
- Notification workflows

□ Establish Breach Response Team

- Privacy Officer
- Security Officer
- Legal counsel
- Public relations
- IT/Security staff

Risk Assessment Process

□ Four-Factor Risk Assessment for each incident:

- Nature and extent of PHI involved
- Unauthorized person who used/received PHI
- Whether PHI was actually acquired or viewed
- Extent to which risk has been mitigated

□ Document all assessments

□ Maintain for 6+ years

Notification Requirements

□ Individual Notification

- Within 60 days of discovery
- First-class mail (or email if agreed)
- Substitute notice if contact info unavailable
- Content requirements met

□ HHS Notification

- Within 60 days for breaches affecting 500+ individuals
- Annual summary for breaches <500 individuals
- Use HHS online reporting tool

□ Media Notification

- Within 60 days for breaches affecting 500+ in a state
- Prominent media outlet in affected area
- Include specific required content

Part 7: Training Requirements

Initial Training

- □ **All new workforce members within reasonable time**
- □ **HIPAA overview and importance**
- □ **Privacy Rule requirements**
- □ **Security Rule requirements**
- □ **Patient rights**
- □ **Incident reporting procedures**
- □ **Sanctions for violations**

Ongoing Training

□ **Annual refresher training for all staff**

□ **Material change training**

(when policies update)

□ **Role-specific training**

- Clinical staff
- Administrative staff
- IT personnel
- Management

□ **Security awareness updates**

- Phishing simulations
- Security bulletins
- Breach examples/lessons learned

Top 10 HIPAA Violations to Avoid

1. □ Failure to conduct organization-wide risk analysis
2. □ Lack of Business Associate Agreements
3. □ Improper disposal of PHI
4. □ Lack of encryption for ePHI
5. □ Employee snooping in medical records
6. □ Denying patient access to records
7. □ Lack of employee training
8. □ Lost or stolen unencrypted devices
9. □ Texting PHI without encryption
10. □ Delayed breach notifications

Annual Compliance Calendar

Frequency	Tasks
Monthly	• Review audit logs • Security awareness reminders • Vulnerability scans • Backup verification • Incident review meeting
Quarterly	• Access control reviews • Policy update reviews • Business Associate check-ins • Compliance metrics reporting • Tabletop exercises
Annual	• Complete Security Risk Assessment • Update all policies and procedures • Conduct workforce training • Test disaster recovery plan • Review and update BAAs • Penetration testing • Compliance program effectiveness review • Submit breach reports (if applicable)

Implementation Tips

1. **Start with a Risk Assessment** - It's the foundation of your compliance program
2. **Document Everything** - If it's not documented, it didn't happen
3. **Train Continuously** - Human error is the biggest risk
4. **Encrypt by Default** - Provides safe harbor in breach situations
5. **Test Your Plans** - Disaster recovery and incident response need regular testing
6. **Review Access Regularly** - Implement least privilege principle
7. **Monitor Constantly** - Use automated tools where possible
8. **Update Frequently** - Regulations and threats evolve
9. **Partner Wisely** - Vet Business Associates thoroughly
10. **Stay Informed** - Subscribe to HHS/OCR updates

Important Resources

Reporting and Compliance

- **HHS Office for Civil Rights (OCR):** www.hhs.gov/ocr
- **Breach Reporting Portal:** ocrportal.hhs.gov
- **HIPAA Complaints:** www.hhs.gov/ocr/privacy/hipaa/complaints

Tools and Guidance

- **Security Risk Assessment Tool:** www.healthit.gov/sra
- **NIST Cybersecurity Framework:** www.nist.gov/cyberframework
- **HIPAA Audit Protocols:** www.hhs.gov/ocr/privacy/hipaa/enforcement/audit

Certification Statement

By completing this checklist, I certify that our organization has:

□ Reviewed all applicable HIPAA requirements

□ Implemented required safeguards

□ Documented our compliance efforts

□ Trained our workforce

□ Established ongoing monitoring procedures

Name: ______________________________

Title: ______________________________

Date: ______________________________

Organization: ______________________________

Need Professional Help?

Achieving HIPAA compliance can be complex. If you need assistance:

Assessment Services: Starting at $5,995

Ongoing Compliance Support: Starting at $2,995/month

Custom Enterprise Solutions: Available

Contact us at **inventivehq.com/contact** to schedule a free HIPAA consultation.

This checklist is provided for informational purposes and should be reviewed by legal counsel and compliance professionals familiar with your specific situation. HIPAA compliance is an ongoing process that requires continuous attention and updates.

Version: 2.0 | **Last Updated:** September 2025 | **Next Review:** September 2026