HIPAA Compliance Checklist

Complete Guide to HIPAA Privacy, Security & Breach Notification Rules

Prepared by PlatOps Security Version 1.0 | January 2026

HIPAA AT A GLANCE

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) establishes national standards to protect individuals' medical records and personal health information (PHI).

Who Must Comply?

1. **Health Plans** - Health insurance companies, HMOs, employer-sponsored plans, government programs
2. **Healthcare Providers** - Doctors, hospitals, pharmacies, nursing homes (who transmit electronically)
3. **Healthcare Clearinghouses** - Entities processing nonstandard health information
4. **Business Associates** - Vendors/contractors accessing PHI on behalf of covered entities

The 3 HIPAA Rules

RULE	FOCUS	KEY REQUIREMENTS
Privacy Rule	Who can access PHI	Patient rights, permitted disclosures, minimum necessary
Security Rule	How to protect ePHI	Administrative, physical, technical safeguards
Breach Notification	What to do if breached	Notify individuals, HHS, and media

 | 4701 Sangamore Road, Suite 100N #2000, Bethesda, MD 20816
hello@platops.com | (202) 864-1197 | platops.com

Civil Monetary Penalties

TIER	VIOLATION TYPE	PER VIOLATION	ANNUAL MAX
Tier 1	Did not know	$100 - $50,000	$25,000
Tier 2	Reasonable cause	$1,000 - $50,000	$100,000
Tier 3	Willful neglect - corrected	$10,000 - $50,000	$250,000
Tier 4	Willful neglect - not corrected	$50,000	$1,500,000

Criminal Penalties

OFFENSE	FINE	IMPRISONMENT
Knowingly obtaining PHI	Up to $50,000	Up to 1 year
Obtaining under false pretenses	Up to $100,000	Up to 5 years
Intent to sell or commercial use	Up to $250,000	Up to 10 years

Key Stat: Average healthcare breach costs $10.9M (highest of any industry)

IMPLEMENTATION TIMELINE

Phase 1: Gap Assessment (4-6 weeks)

- [ ] Inventory all systems with ePHI
- [ ] Identify all PHI data flows
- [ ] Conduct initial risk assessment
- [ ] Review existing policies and procedures
- [ ] Identify gaps in current controls
- [ ] Prioritize remediation efforts

Phase 2: Policy Development (4-8 weeks)

- [ ] Develop HIPAA policies and procedures
- [ ] Create Notice of Privacy Practices
- [ ] Draft Business Associate Agreements
- [ ] Establish incident response procedures
- [ ] Document workforce sanctions policy
- [ ] Create contingency/disaster recovery plans

Phase 3: Technical Implementation (8-16 weeks)

- [ ] Implement access controls and MFA
- [ ] Deploy encryption (at rest and in transit)
- [ ] Configure audit logging and monitoring
- [ ] Establish backup and recovery systems

 | 4701 Sangamore Road, Suite 100N #2000, Bethesda, MD 20816
hello@platops.com | (202) 864-1197 | platops.com

- [ ] Train on role-specific procedures
- [ ] Document training completion
- [ ] Establish ongoing training program
- [ ] Distribute Notice of Privacy Practices

Phase 5: Validation & Maintenance (Ongoing)

- [ ] Conduct internal audits
- [ ] Perform annual risk assessments
- [ ] Update policies as needed
- [ ] Monitor for regulatory changes
- [ ] Maintain documentation
- [ ] Consider third-party assessment

Total Timeline: 6-12 months for full implementation

ADMINISTRATIVE SAFEGUARDS

Administrative safeguards are policies and procedures to manage selection, development, and maintenance of security measures.

Security Management (4 items) - REQUIRED

- [ ] Conduct comprehensive risk analysis
- [ ] Implement risk management program
- [ ] Apply appropriate sanctions for violations
- [ ] Review system activity regularly (audit logs)

Assigned Security Responsibility (1 item) - REQUIRED

- [ ] Designate a security official responsible for HIPAA compliance

Workforce Security (3 items) - REQUIRED

- [ ] Implement authorization procedures
- [ ] Establish workforce clearance procedures
- [ ] Define termination procedures (access revocation within 24 hours)

Information Access Management (3 items) - REQUIRED

- [ ] Isolate healthcare clearinghouse functions (if applicable)
- [ ] Implement access authorization policies
- [ ] Establish access modification procedures

Security Awareness Training (4 items) - REQUIRED

- [ ] Conduct security reminders (periodic)
- [ ] Provide malware protection training
- [ ] Implement login monitoring

- [ ] Document all security incidents

Contingency Planning (5 items) - REQUIRED

- [ ] Create data backup plan
- [ ] Develop disaster recovery plan
- [ ] Establish emergency mode operation plan
- [ ] Test and revise procedures (annually)
- [ ] Assess criticality of applications and data

Evaluation (1 item) - REQUIRED

- [ ] Perform periodic security evaluations (at least annually)

Business Associate Contracts (2 items) - REQUIRED

- [ ] Execute BAAs with all business associates
- [ ] Include required contract provisions (see Page 11)

Administrative Safeguards Total: 25 items

PHYSICAL SAFEGUARDS

Physical safeguards are physical measures to protect electronic information systems and related buildings.

Facility Access Controls (4 items) - REQUIRED

- [ ] Implement contingency operations procedures
- [ ] Develop facility security plan
- [ ] Establish access control procedures (badges, keys, biometrics)
- [ ] Maintain maintenance records

Workstation Use (2 items) - REQUIRED

- [ ] Define appropriate workstation use policies
- [ ] Document workstation security requirements

Workstation Security (2 items) - REQUIRED

- [ ] Implement physical safeguards for workstations
- [ ] Restrict workstation access to authorized users

Device and Media Controls (4 items) - REQUIRED

- [ ] Establish disposal procedures (secure data destruction)
- [ ] Implement media re-use procedures
- [ ] Maintain accountability records
- [ ] Create data backup and storage procedures

Technical safeguards are technology and policies to protect and control access to ePHI.

Access Control (4 items) - REQUIRED

- [ ] Assign unique user identification
- [ ] Establish emergency access procedures
- [ ] Implement automatic logoff (15 minutes max recommended)
- [ ] Implement encryption and decryption (AES-256)

Audit Controls (3 items) - REQUIRED

- [ ] Implement audit logging mechanisms
- [ ] Record and examine system activity
- [ ] Retain audit logs appropriately (6 years recommended)

Integrity Controls (2 items) - REQUIRED

- [ ] Implement mechanism to authenticate ePHI
- [ ] Protect ePHI from improper alteration/destruction

Person or Entity Authentication (2 items) - REQUIRED

- [ ] Verify identity of users seeking access
- [ ] Implement multi-factor authentication (MFA)

Transmission Security (2 items) - REQUIRED

- [ ] Implement integrity controls for transmission
- [ ] Implement encryption for transmission (TLS 1.2+)

Technical Safeguards Total: 13 items

PRIVACY RULE REQUIREMENTS

The Privacy Rule establishes standards for protecting medical records and PHI.

Patient Rights (6 items)

- [ ] Right to access their PHI
- [ ] Right to request amendments to PHI
- [ ] Right to accounting of disclosures
- [ ] Right to request restrictions on disclosures
- [ ] Right to confidential communications
- [ ] Right to file complaints

Covered Entity Obligations (8 items)

- [ ] Publish Notice of Privacy Practices

- [ ] Designate privacy official
- [ ] Train workforce on privacy practices
- [ ] Apply sanctions for violations

Permitted Uses and Disclosures (5 items)

- [ ] Document treatment, payment, healthcare operations (TPO)
- [ ] Document public health activities
- [ ] Document required law enforcement disclosures
- [ ] Document abuse/neglect reporting requirements
- [ ] Document research authorizations

Privacy Rule Total: 19 items

BREACH NOTIFICATION REQUIREMENTS

What Constitutes a Breach?

A breach is unauthorized acquisition, access, use, or disclosure of PHI that compromises security or privacy, UNLESS:

- Unintentional acquisition by workforce member acting in good faith
- Inadvertent disclosure between authorized persons
- Recipient unable to retain the information

Notification Requirements

AFFECTED	NOTIFICATION	DEADLINE	METHOD
Individuals	Always required	60 days from discovery	Written mail (or email if agreed)
HHS (< 500)	Annual report	Within 60 days of calendar year end	HHS web portal
HHS (500+)	Immediate	Within 60 days of discovery	HHS web portal
Media (500+)	Required	Within 60 days	Local media in affected state

Breach Documentation (4 items)

- [ ] Document all potential breaches
- [ ] Conduct risk assessment for each incident
- [ ] Maintain breach investigation records
- [ ] Track notification compliance

Breach Content Requirements (6 items)

- [ ] Description of what happened
- [ ] Types of PHI involved
- [ ] Steps individuals should take
- [ ] What you're doing to investigate
- [ ] What you're doing to mitigate harm
- [ ] Contact information for questions

BAA Must Include These 12 Provisions:

- [ ] Describe permitted uses and disclosures of PHI
- [ ] Prohibit uses/disclosures not in agreement or by law
- [ ] Require appropriate safeguards for PHI
- [ ] Require reporting of unauthorized uses or disclosures
- [ ] Require subcontractors to agree to same restrictions
- [ ] Make PHI available for individual access rights
- [ ] Make PHI available for amendment requests
- [ ] Provide accounting of disclosures
- [ ] Make practices available to HHS for compliance review
- [ ] Return or destroy PHI at termination
- [ ] Authorize termination for material breach
- [ ] Require breach notification to covered entity

BAA Management (4 items)

- [ ] Maintain inventory of all business associates
- [ ] Track BAA execution dates and renewal
- [ ] Conduct periodic BA compliance reviews
- [ ] Update BAAs when regulations change

COMMON PITFALLS

1. Incomplete Risk Analysis

Problem: Superficial assessment misses critical vulnerabilities. **Solution:** Conduct comprehensive risk analysis covering ALL ePHI systems.

2. Missing Business Associate Agreements

Problem: No BAAs with vendors accessing PHI - most common audit finding. **Solution:** Inventory all vendors and execute BAAs before sharing data.

3. Inadequate Training

Problem: Generic or infrequent training. Human error causes most breaches. **Solution:** Role-specific training at hire and annually with documented completion.

4. No Encryption

Problem: Unencrypted ePHI on laptops/mobile = reportable breach if lost. **Solution:** Encrypt all ePHI at rest (AES-256) and in transit (TLS 1.2+).

5. Poor Access Controls

Problem: Shared accounts, excessive permissions, no MFA. **Solution:** Unique IDs, RBAC, MFA, regular access reviews, prompt termination.

6. Lack of Audit Logs

Total Controls by Category

CATEGORY	ITEMS	STATUS
Administrative Safeguards	25	Required
Physical Safeguards	12	Required
Technical Safeguards	13	Required
Privacy Rule	19	Required
Breach Notification	10	Required
BAA Requirements	16	Required
TOTAL	**95**	

Your Readiness Score

Scoring Guide:

- 0-25% Complete: Critical - Significant gaps exist
- 26-50% Complete: At Risk - Major remediation needed
- 51-75% Complete: In Progress - Continue implementation
- 76-90% Complete: Nearly Ready - Focus on documentation
- 91-100% Complete: Compliant - Maintain and monitor