LITSLINK HEALTHCARE

HIPAA Technical Safeguards Checklist 2026

For healthcare applications handling
Protected Health Information (PHI)

22+
Checklist Items

7
Security Categories

2026
Updated Standards

Provided by LITSLINK, a HIPAA-compliant development partner
trusted by US-based providers, payers, and HealthTech companies.

litslink.com

What Is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a federal statute enforced by the United States government to safeguard the confidentiality and security of patient data. It ensures that stored, processed, and transmitted protected health information (PHI), including electronic PHI (ePHI), is secured. As of 2026, HIPAA compliance is more critical than ever with the rise of AI, IoT devices, and telehealth platforms in healthcare.

HIPAA Privacy Rule

Gives patients control over their medical data by setting limits for using and disclosing PHI without their authorization.

HIPAA Security Rule

Establishes standards for protecting ePHI when it's stored or shared to ensure confidentiality, integrity, and availability.

HIPAA Breach Notification Rule

Requires covered entities to notify affected patients promptly if unsecured ePHI is breached.

HIPAA Enforcement Rule

Clarifies penalties for HIPAA violations, including penalties for violations of the Privacy, Security, and Breach Notification Rules.

Why HIPAA Compliance Matters

$363
Average cost per breached record

80%
Of healthcare orgs fail meaningful use audit

~600
HIPAA violations referred to DOJ

$50K
Maximum fine per serious HIPAA violation

$1.5M
Annual penalty cap for repeated violations

1 in 4
HIPAA breaches go unreported

Failing to Comply With HIPAA

Failing to comply with HIPAA rules can have serious consequences — from significant financial penalties to criminal charges and reputational damage. The Office for Civil Rights (OCR) at HHS actively enforces HIPAA and has collected over $130M in settlements and penalties from covered entities and business associates.

Tier 1 — No Knowledge

$145 – $73,011 per violation · Annual cap: $25,000 per provision

You had no knowledge of the violation and, with reasonable diligence, could not have known it occurred.

Tier 2 — Reasonable Cause

$1,461 – $73,011 per violation · Annual cap: $100,000 per provision

You knew or should have known of the violation through reasonable diligence, but it was not willful neglect.

Tier 3 — Willful Neglect (Corrected)

$14,602 – $73,011 per violation · Annual cap: $250,000 per provision

The violation resulted from willful neglect of HIPAA rules but was corrected within 30 days of discovery.

Tier 4 — Willful Neglect (Not Corrected)

$73,011+ per violation · Annual cap: up to $2,190,294 per provision

The violation resulted from willful neglect and was NOT corrected within the required 30-day period — the most severe penalty.

Key Enforcement Statistics

$2.19M
Maximum annual penalty per provision (2025)

$73K
Maximum fine per single violation

10 yrs
Maximum criminal sentence (malicious)

$16.1M
Largest HIPAA settlement OCR, 2024

60 days
Breach notification deadline to HHS

1 in 4
HIPAA breaches go unreported

For full details on HIPAA enforcement, visit the official HHS resource:
https://www.hhs.gov/hipaa/for-professionals/index.html

Key HIPAA Updates for 2026

The HIPAA Security Rule updates finalized in 2025–2026 strengthen standards and implementation specifications by introducing new requirements and clarifying existing ones. These changes reflect the evolving threat landscape and the growing adoption of AI and IoT in healthcare.

Strengthening Cybersecurity Measures

HHS has moved to eliminate the distinction between "required" and "addressable" implementation specifications, making all standards mandatory. This ensures consistent application of cybersecurity measures across all covered entities and business associates.

AI and Machine Learning Safeguards

New guidance addresses the use of AI/ML systems that process ePHI, including requirements for algorithmic transparency, bias auditing, and secure model training pipelines. Organizations using AI-powered diagnostics or analytics must document data flows and access controls.

Aligning with 42 CFR Part 2

Regulations for the confidentiality of Substance Use Disorder and Mental Health Services Administration patient records are now better aligned with HIPAA standards, enhancing care coordination and simplifying compliance for entities managing both types of sensitive information.

HIPAA and Reproductive Health

Revised conditions govern when PHI related to reproductive healthcare can be used or disclosed. These modifications reflect evolving legal and social considerations, ensuring healthcare providers can share PHI that aligns with patients' rights.

Enhanced Breach Notification Requirements

Shorter notification timelines and expanded reporting obligations for breaches affecting fewer than 500 individuals. Organizations must now report to HHS within 60 days for all breach sizes, with stricter documentation of remediation steps taken.

Technical Safeguards Checklist

Note: This checklist covers the key technical safeguards required or addressable under the HIPAA Security Rule (45 CFR Part 164, Subpart C). Items marked **Required** have no flexibility under the Security Rule. Items marked **Addressable** must be implemented if reasonable and appropriate — or the decision not to implement must be documented with an equivalent alternative.

ACCESS CONTROLS

- [ ] **Unique user identification** — Required

  Each user must have a unique login. Shared credentials are a HIPAA violation and a security risk. Enforce unique usernames at the application layer.

- [ ] **Automatic session timeout** — Required

  Sessions accessing PHI must time out after inactivity. Recommended: 15 minutes for clinical workstations, 5 minutes for mobile devices in clinical settings.

- [ ] **Role-based access control (RBAC)** — Required

  Access to PHI should be limited to the minimum necessary for each role. Implement role definitions at the data model level, not just the UI layer.

- [ ] **Emergency access procedure** — Required

  A documented procedure must exist for accessing PHI in emergencies when normal authentication isn't possible. This access must be logged and reviewed.

AUDIT CONTROLS

- [ ] **Audit logging for all PHI access** — Required

  Every read, write, modify, and delete operation on PHI must be logged with timestamp, user ID, action type, and record identifier. Logs must be tamper-evident.

- [ ] **Audit log retention (minimum 6 years)** — Required

  HIPAA requires retention of policies and procedures for 6 years. Audit logs should be retained for at least this period. Store logs in a separate, secured environment.

- [ ] **Regular log review process** — Addressable

  Audit logs are useless without a review cadence. Document who reviews logs, how often, and what triggers an escalation. Automated alerting helps but doesn't replace review.

TRANSMISSION SECURITY

- [ ] **TLS 1.3 for all PHI in transit** — Required

  All API calls, web sessions, and data transfers involving PHI must use TLS 1.3 (or minimum TLS 1.2). TLS 1.0 and 1.1 are deprecated. Enforce HTTPS-only with HSTS headers.

- [ ] **End-to-end encryption for messaging** — Required

  If your application supports secure messaging between clinicians or between clinician and patient, messages containing PHI must be encrypted end-to-end — not just in transit.

- [ ] **VPN or equivalent for internal networks** — Addressable

  Any internal network transmission of PHI (e.g., between application servers and databases) should use encrypted channels, not plain internal network traffic.

DATA ENCRYPTION & STORAGE

- [ ] **PHI encrypted at rest (AES-256)** — Required

  All PHI stored in databases, file systems, backups, and caches must be encrypted at rest using AES-256 or equivalent. This includes database backups and exported reports.

- [ ] **Encryption key management** — Required

  Encryption keys must be stored separately from the encrypted data, rotated on a defined schedule, and access-controlled. Key compromise means data compromise.

- [ ] **PHI de-identification for analytics** — Addressable

  When using PHI data for analytics, reporting, or ML training, apply Safe Harbor or Expert Determination de-identification methods. De-identified data is no longer subject to HIPAA.

- [ ] **Secure local and mobile storage** — Required

  PHI stored on mobile devices must use platform-native secure storage (iOS Keychain, Android Keystore). No PHI in push notification content, logs, screenshots, or clipboard.

INTEGRITY CONTROLS

- [ ] **Data integrity validation** — Addressable

  Implement mechanisms to ensure PHI has not been improperly altered or destroyed. This includes checksums, database transaction integrity, and version history for critical records.

- [ ] **Backup and disaster recovery plan** — Required

  A documented, tested backup and recovery plan is required. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) must be defined and tested at least annually.

- [ ] **Backup restore verification** — Required

  Encrypted backups must be configured and restore tested at least quarterly. Verify that restored data matches expected integrity checksums and is fully functional.

AUTHENTICATION & IDENTITY

- [ ] **Multi-factor authentication (MFA)** — Required

  Administrative access to systems containing PHI must require MFA. Strongly recommended for all clinical user access. Time-based OTP (TOTP) or hardware keys preferred.

- [ ] **Secure password policy enforcement** — Required

  Minimum length (12+ characters), complexity requirements, breach-list checking (HaveIBeenPwned API), and no password hints. Password managers should be encouraged, not blocked.

- [ ] **OAuth 2.0 / SMART on FHIR for API auth** — Required

  If your application exposes APIs that access PHI, use OAuth 2.0 with PKCE for authorization. SMART on FHIR is the standard for EHR-integrated applications.

- [ ] **Brute-force protection** — Required

  Rate limits, account lockouts, and monitoring must be in place to prevent credential-stuffing and brute-force attacks on authentication endpoints.

VENDOR & BUSINESS ASSOCIATE MANAGEMENT

- [ ] **BAA executed with all PHI-touching vendors** — Required

  Any vendor, cloud provider, or subcontractor that handles PHI on your behalf must have a signed Business Associate Agreement. This includes AWS, Google Cloud, and Azure.

- [ ] **Vendor security review cadence** — Addressable

  Document how you assess the security posture of business associates, how often reviews happen, and what triggers re-evaluation. A BAA is not a one-time check.

- [ ] **Third-party/vendor inventory maintained** — Required

  Maintain a current inventory of all vendors, APIs, SDKs, and subcontractors that have any access to PHI. Review and update this inventory at least annually.

APPLICATION & API SECURITY

- [ ] **Authorization enforced on every endpoint** — Required

  Every API endpoint must enforce authorization checks. Prevent IDOR exposure by validating that the authenticated user has permission to access the requested resource.

- [ ] **Input validation and output sanitization** — Required

  All user inputs must be validated and sanitized. Implement protections against SQL injection, XSS, CSRF, and other OWASP Top 10 vulnerabilities.

- [ ] **Incident response plan defined** — Required

  Incident severity levels, escalation paths, and response contacts must be documented. Conduct tabletop exercises at least annually to test response readiness.

- [ ] **Security scan results reviewed** — Addressable

  SAST/DAST or equivalent security scans must be performed before major releases. Review and remediate findings before deploying to production.

LITSLINK HEALTHCARE

22+
Checklist Items

7
Security Categories

2026
Updated Standards

Security readiness is a continuous process, not a one-time milestone.

As your healthcare app evolves — new workflows, integrations, and user roles — your security posture should evolve with it.

Need help implementing these controls?

LITSLINK builds HIPAA-compliant healthcare software for US-based providers, payers, and HealthTech companies.

litslink.com/contact-us

Free consultation
48h response guaranteed