



HIPAA Compliance Checklist: Healthcare Data Security

Privacy Rule Assessment

Evaluate adherence to HIPAA Privacy Rule requirements, including Notice of Privacy Practices and patient rights.

Last Updated Notice of Privacy Practices (NPP)

Is NPP readily available to patients?

- ☐ Yes
- ☐ No
- ☐ Partially

Summary of Patient Rights (as outlined in NPP)

Are patient requests for access to records handled within the required timeframe?

- ☐ Yes
- ☐ No
- ☐ Occasionally

Number of patient complaints related to privacy practices in the last year

Enter a number...

Description of process for patients to submit privacy concerns

Write something...

Are patient authorizations for uses/disclosures reviewed and validated?

- ☐ Yes
- ☐ No
- ☐ Occasionally

Security Rule Implementation

Verify the implementation of administrative, physical, and technical safeguards outlined in the Security Rule.

Security Risk Assessment Completed?

- ☐ Yes
- ☐ No
- ☐ In Progress

Last Security Rule Review Date

Enter date...

Number of Systems Covered by Security Rule

Enter a number...


Summary of Security Rule Implementation Gaps Identified

Write something...

Implemented Security Safeguards (Select All That Apply)

- ☐ Administrative Safeguards
- ☐ Physical Safeguards
- ☐ Technical Safeguards

Supporting Documentation (e.g., security policies)

 Upload File

Encryption at Rest Implemented?

- ☐ Yes
- ☐ No
- ☐ Partial

Business Associate Agreements (BAA)

Confirm all Business Associate Agreements are in place, current, and compliant with HIPAA regulations.

BAA Expiration Date

- ☐ Within 30 days
- ☐ Within 60 days
- ☐ Within 90 days
- ☐ Beyond 90 days

Last BAA Review Date

Enter date...

Summary of BAA Scope

Write something...

Copy of Business Associate Agreement

 Upload File

BAA Status

- ☐ Active
- ☐ Inactive
- ☐ Renewal Pending

Business Associate Name

Write something...

Contract Value (Optional)

Enter a number...

Risk Analysis & Management

Review the most recent Risk Analysis and associated remediation plan.

Date of Last Risk Analysis

Enter date...

Summary of Risk Analysis Findings

Write something...

Number of Identified Risks

Enter a number...

Risk Categories Assessed (e.g., Technical, Administrative, Physical)

- ☐ Technical
- ☐ Administrative
- ☐ Physical
- ☐ Legal/Regulatory


Description of Key Mitigation Strategies Implemented

Write something...

Date of Next Scheduled Risk Analysis Review

Enter date...

Upload of Risk Analysis Documentation

 Upload File

Data Access Controls

Validate appropriate access controls are in place for electronic protected health information (ePHI).

Access Control Method Implemented?

- ☐ Role-Based Access Control (RBAC)
- ☐ Attribute-Based Access Control (ABAC)
- ☐ Access Control Lists (ACLs)
- ☐ Other (Specify)

Number of Users with 'Administrator' Access

Enter a number...

Which data categories are restricted with access controls?

- ☐ Patient Demographics
- ☐ Medical History
- ☐ Billing Information
- ☐ Lab Results
- ☐ Medication Records

Date of Last Access Control Review

Enter date...

Is Two-Factor Authentication (2FA) implemented for all users accessing ePHI?

- ☐ Yes
- ☐ No
- ☐ Partial Implementation

Describe any exceptions to standard access control policies and justification.

Write something...

Encryption & Data Transmission

Confirm ePHI is encrypted both in transit and at rest.

Encryption Method for Data at Rest

- ☐ AES-256
- ☐ Triple DES
- ☐ Other (Specify)

Encryption Method for Data in Transit

- ☐ TLS 1.2 or higher
- ☐ SSL 3.0 (Not Recommended)
- ☐ Other (Specify)

Encryption Key Rotation Frequency (in days)

Enter a number...

Describe Key Management Process

Write something...

Data Transmission Method

- ☐ Secure FTP
- ☐ HTTPS
- ☐ Other (Specify)

Last Encryption Policy Review Date

Enter date...

Incident Response Plan

Assess the readiness and effectiveness of the incident response plan for potential HIPAA breaches.

Date of Last Incident Response Plan Review

Enter date...

Summary of Recent Plan Updates/Changes

Write something...

Primary Contact for Incident Response

- ☐ Security Officer
- ☐ Compliance Officer
- ☐ IT Director
- ☐ Legal Counsel

Number of Staff Trained on Incident Response

Enter a number...

Incident Types Covered by Plan

- ☐ Malware Infection
- ☐ Data Breach
- ☐ Unauthorized Access
- ☐ Lost Device
- ☐ Phishing Attack

Description of Post-Breach Notification Procedures

Write something...

Supporting Documentation (e.g., notification templates)

 Upload File

Employee Training & Awareness

Verify employees receive regular HIPAA training and demonstrate understanding of regulations.

Last Training Completion Date

Enter date...

Training Module Covered

- ☐ Privacy Rule
- ☐ Security Rule
- ☐ Breach Notification Rule
- ☐ Physical Safeguards
- ☐ Administrative Safeguards
- ☐ Technical Safeguards

Topics Covered in Training (Select All That Apply)

- ☐ ePHI Handling
- ☐ Password Security
- ☐ Phishing Awareness
- ☐ Breach Reporting
- ☐ Data Access Protocols

Score on Training Assessment (if applicable)

Enter a number...

Employee Comments/Feedback on Training

Write something...

Training Format

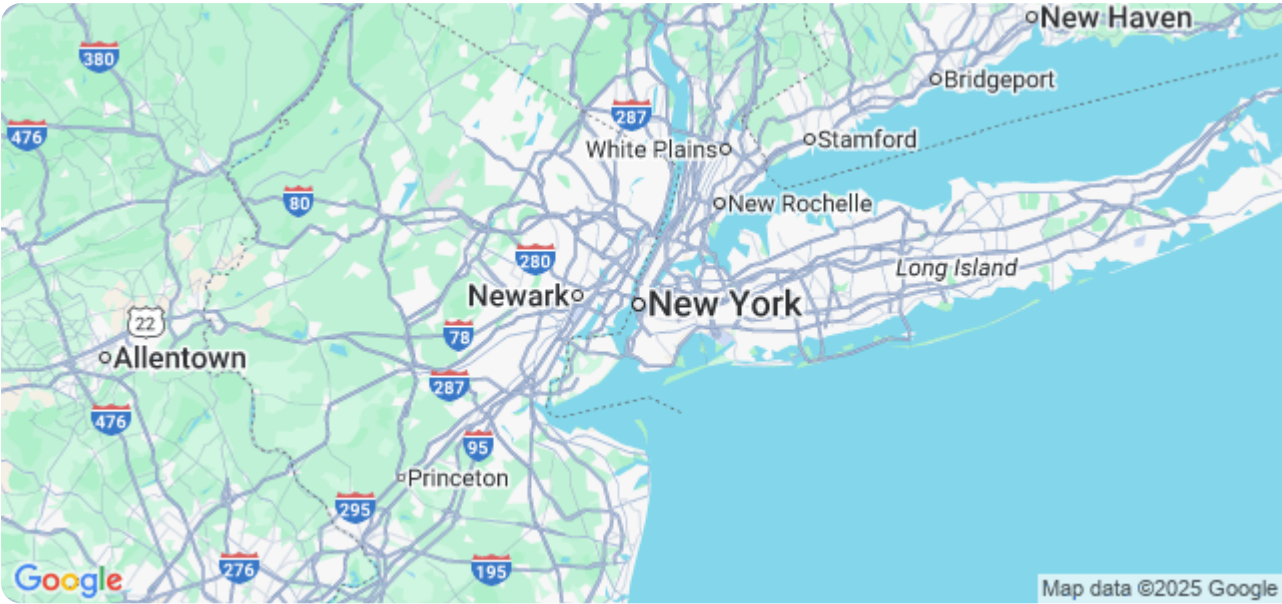
- ☐ Online Module
- ☐ In-Person Session
- ☐ Webinar

Physical Security Measures

Evaluate the adequacy of physical security measures to protect ePHI.

Server Room Location

 Set My Current Location



Security System Type

- ☐ Keycard Access
- ☐ Biometric Scanning
- ☐ Security Personnel
- ☐ None

Number of Security Cameras

Enter a number...

Visitor Management System

- ☐ Implemented
- ☐ Partially Implemented
- ☐ Not Implemented

Date of Last Physical Security Audit

Enter date...

Description of Emergency Exit Procedures

Write something...

Audit Trails & Monitoring

Review audit trail configurations and system monitoring processes for detecting unauthorized access.

Audit Log Retention Period (in days)

Enter a number...

Audit Logging Level

- ☐ Minimal
- ☐ Standard
- ☐ Detailed

Last Audit Log Review Date

Enter date...

Summary of Audit Log Review Findings

Write something...

Systems with Active Audit Trails

- ☐ Electronic Health Record (EHR)
- ☐ Practice Management System
- ☐ Billing System
- ☐ Network Infrastructure
- ☐ Remote Access Servers

Frequency of Automated Audit Report Generation