ChecklistGuro

Healthcare IT Security Checklist: Data Protection & Access Control

Data Encryption & Storage

Ensuring sensitive patient data is protected both at rest and in transit.

Encryption Method Used (Data at Rest)

□ AES-256

□ Triple DES

□ Other (Specify)

Encryption Method Used (Data in Transit)

□ TLS 1.2 or higher

□ SSL 3.0

□ Other (Specify)

Encryption Key Rotation Frequency (Days)

Enter a number...

Description of Data Storage Location(s)

Write something...

Data Masking Implemented?

□ Yes
□ No
□ Partial

Encryption Key Management Policy Document

Upload File

Access Control & Authentication

Managing user permissions and verifying identities.

Multi-Factor Authentication Enabled?

□ Yes
□ No
□ Partial Implementation

Password Complexity Requirements Applied?

□ Yes
□ No
□ Review Required

Maximum Password Age (Days)

Enter a number...

Privilege Access Review Frequency

□ Monthly

□ Quarterly

□ Annually

□ Ad-Hoc

Role-Based Access Control (RBAC) Implemented for:

□ EHR/EMR

□ Financial Systems

□ Laboratory Information Systems

□ Imaging Systems

□ Other (Specify)

Last Access Control Audit Date

Enter date...

Notes on Access Control Processes

Write something...

Network Security

Protecting network infrastructure from unauthorized access and threats.

Firewall Status

□ Active

□ Inactive

□ Maintenance Mode

Firewall Rule Count

Enter a number...

Intrusion Detection System (IDS) Status

- □ Active
- □ Inactive
- □ Alerts Pending Review

Recent Network Activity Logs Summary

Write something...

VPN Status

- □ Enabled
- □ Disabled
- □ Active Connections: 0

Last Network Security Scan Date

Enter date...

Network Segmentation Implemented?

- □ VLANs
- □ Microsegmentation
- □ Firewall Rules
- □ None

Endpoint Security

Securing devices accessing healthcare data, including computers, tablets, and mobile phones.

Endpoint Protection Software Installed?

□ Yes

□ No

□ N/A

Last Full Scan Completion Status (0 = Failed, 1 = Passed)

Enter a number...

Last Security Patch Applied Date

Enter date...

Mobile Device Management (MDM) implemented?

□ Yes

□ No

□ N/A

Which of the following endpoint security controls are in place?

□ Antivirus Software

□ Firewall

□ Data Loss Prevention (DLP)

□ Disk Encryption

□ Remote Wipe Capability

Describe any unusual endpoint behavior observed recently.

Write something...

Vulnerability Management

Identifying and mitigating security vulnerabilities in systems and applications.

Last Vulnerability Scan Date

Enter date...

Scan Frequency (Days)

Enter a number...

Summary of Recent Scan Results

Write something...

Critical/High Severity Vulnerabilities Found?

- □ Yes
- □ No
- □ Pending Scan

Description of Remediation Steps for High Severity Vulnerabilities

Write something...

Target Remediation Completion Date

Enter date...

Vulnerability Scanning Tool Used

□ Nessus

□ Qualys

□ Rapid7

□ Other

Scan Report Attachment (Optional)

Upload File

Incident Response & Recovery

Planning for and responding to security incidents effectively.

Incident Start Date/Time

Enter date...

Brief Description of Incident

Write something...

Incident Severity (Low, Medium, High, Critical)

□ Low

□ Medium

□ High

□ Critical

Estimated Number of Records Affected

Enter a number...

Systems Impacted (Check all that apply)

□ EHR

□ Billing System

□ Patient Portal

□ Network Infrastructure

Containment Steps Taken

Write something...

Eradication Steps Taken

Write something...

Date of Recovery Confirmation

Enter date...

Backup and Disaster Recovery

Implementing strategies to ensure data availability in case of system failures or disasters.

Backup Frequency (e.g., Daily, Weekly)

Enter a number...

Last Successful Full Backup Date

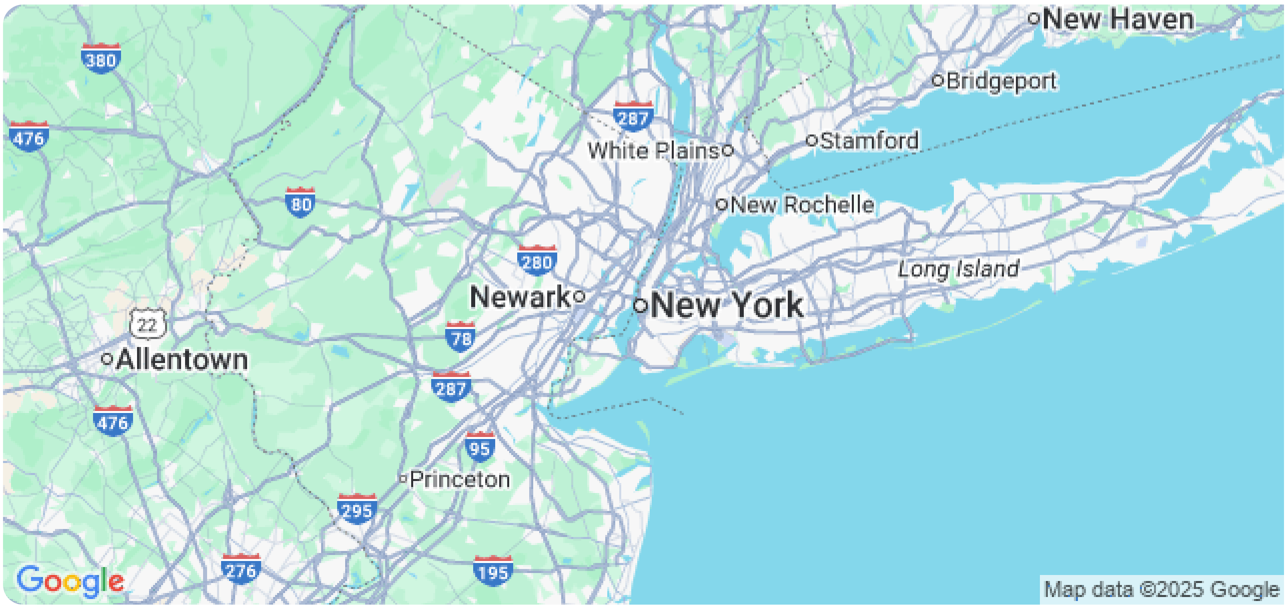
Enter date...

Retention Period for Backups (in days)

Enter a number...

Offsite Backup Storage Location

Set My Current Location



Backup Verification Method (e.g., Test Restore)

☐ Test Restore

☐ File Integrity Check

☐ Automated Verification

Last Disaster Recovery Drill Date

Enter date...

Detailed Description of Disaster Recovery Plan

Write something...

Security Awareness Training

Educating staff on security best practices and potential threats.

Last Training Completion Date

□ Within Last 3 Months

□ 3-6 Months Ago

□ 6-12 Months Ago

□ Over 12 Months Ago

Topics Covered in Training

□ Phishing Recognition

□ Password Security

□ HIPAA Compliance

□ Malware Prevention

□ Data Breach Reporting

□ Physical Security

Briefly describe your understanding of phishing scams.

Write something...

How do you typically report suspected phishing emails?

□ To IT Security Department

□ To Supervisor

□ Delete and Ignore

How many times have you reviewed the organization's security policies this year?

Enter a number...

Compliance & Regulatory Requirements

Adhering to relevant laws and regulations, such as HIPAA and HITECH.

HIPAA Security Rule Assessment Completed?

□ Yes

□ No

□ In Progress

Last HIPAA Risk Assessment Date

Enter date...

State Privacy Law Compliance?

□ Applicable - Yes

□ Applicable - No

□ Unknown

Summary of Relevant State Privacy Laws Applied

Write something...

HITECH Act Compliance?

□ Yes

□ No

□ N/A

Breach Notification Reporting Deadline (Days)

Enter a number...

Supporting Documentation (e.g., Policies, Agreements)

Upload File

Third-Party Risk Management

Assessing and managing security risks associated with third-party vendors.

Vendor Risk Tier (High, Medium, Low)

□ High

□ Medium

□ Low

Vendor Contract Start Date

Enter date...

Last Risk Assessment Completion Date

Enter date...

Number of Patients' Data Processed by Vendor

Enter a number...

Summary of Vendor's Security Practices

Write something...

Services Provided by Vendor (Select all that apply)

□ Data Storage
□ Data Processing
□ Software Development
□ IT Support
□ Other

Vendor Security Assessment Report

Upload File

Vendor Compliance Status (Compliant, Non-Compliant, In Progress)

□ Compliant
□ Non-Compliant
□ In Progress