ChecklistGuro

Healthcare Cybersecurity Incident Response Checklist

Detection & Identification

Initial steps to recognize and confirm a potential cybersecurity incident.

Date of Suspected Incident

Enter date...

Time of Suspected Incident

Initial Detection Method

- □ Antivirus Alert
- □ Intrusion Detection System (IDS)
- □ User Report
- □ Network Monitoring
- □ Security Information and Event Management (SIEM)

Description of Initial Alert/Observation

Write something...

Affected System(s) - Initial Assessment

□ Server

□ Workstation

□ Network Device

□ Database

□ Web Application

□ Unknown

Severity Score (if applicable)

Enter a number...

Potential Indicators of Compromise (IOCs)

□ Malware Signature Detected

□ Unusual Network Traffic

□ Suspicious User Activity

□ Unauthorized File Access

□ Unexpected System Changes

Containment

Actions to limit the scope and impact of the incident.

Affected System Type

□ Server

□ Workstation

□ Network Device

□ Mobile Device

□ Application

Compromised Services

- □ Email
- □ File Server
- □ Database
- □ Web Application
- □ VPN

Number of Affected Users (Estimate)

Enter a number...

Date System Isolated

Enter date...

Time System Isolated

Detailed Description of Isolation Actions

Write something...

Isolation Method

- □ Network Disconnect
- □ Firewall Rule
- □ System Shutdown

Eradication

Removing the threat actor, malicious code, or vulnerability from the system.

Description of Malware/Threat Actor

Write something...

Number of Affected Systems Initially

Enter a number...

Compromised System Roles (e.g., Server, Workstation)

- □ Server
- □ Workstation
- □ Database
- □ Network Device

Malware Sample (if available)

Upload File

Detailed Removal Steps Performed

Write something...

Date Eradication Steps Completed

Enter date...

Time Eradication Steps Completed

Recovery

Restoring affected systems and data to normal operation.

System Restoration Start Date

Enter date...

System Restoration Start Time

Number of Affected Systems Restored

Enter a number...

Detailed Description of Restoration Process

Write something...

Data Integrity Verification Method

□ Automated Verification

□ Manual Spot Checks

□ Full Data Reconciliation

Date of Full System Validation

Enter date...

Signature of Recovery Team Lead

Post-Incident Activity

Reviewing the incident, documenting lessons learned, and implementing corrective actions.

Detailed Incident Narrative

Write something...

Estimated Financial Impact (USD)

Enter a number...

Root Cause Categories

- ☐ Technical Vulnerability
- ☐ Human Error
- ☐ Process Failure
- ☐ Third-Party Risk

Date of Incident Report Completion

Enter date...

Proposed Corrective Actions

Write something...

Action Plan Status

□ Not Started
□ In Progress
□ Completed
□ Delayed

Supporting Documentation (Logs, Screenshots)

Upload File

Communication & Reporting

Internal and external communication protocols and reporting requirements.

Incident Severity Level

□ Low
□ Medium
□ High
□ Critical

Summary of Communication Actions Taken

Write something...

Number of Individuals Notified (Internal)

Enter a number...

Number of Individuals Notified (External)

Enter a number...

Date of Initial Notification

Enter date...

Time of Initial Notification

Primary Communication Channel Used

□ Email
□ Phone
□ Secure Messaging
□ Other

Notes on Communication Effectiveness

Write something...

Legal & Regulatory Compliance

Ensuring adherence to relevant laws, regulations, and contractual obligations (e.g., HIPAA breach notification).

Breach Notification Triggered?

□ Yes

□ No

Date of Breach Discovery

Enter date...

Estimated Number of Records Affected

Enter a number...

Summary of Legal Consultation Performed

Write something...

State Breach Notification Laws Applicable?

□ Yes

□ No

Documentation of Legal Review

Upload File

Description of steps taken to comply with HIPAA Breach Notification Rule

Write something...