



Healthcare Data Breach Response Checklist: Notification & Remediation

Containment & Assessment

Immediate steps to limit damage and understand the scope of the breach.

Date Breach Detected

Enter date...

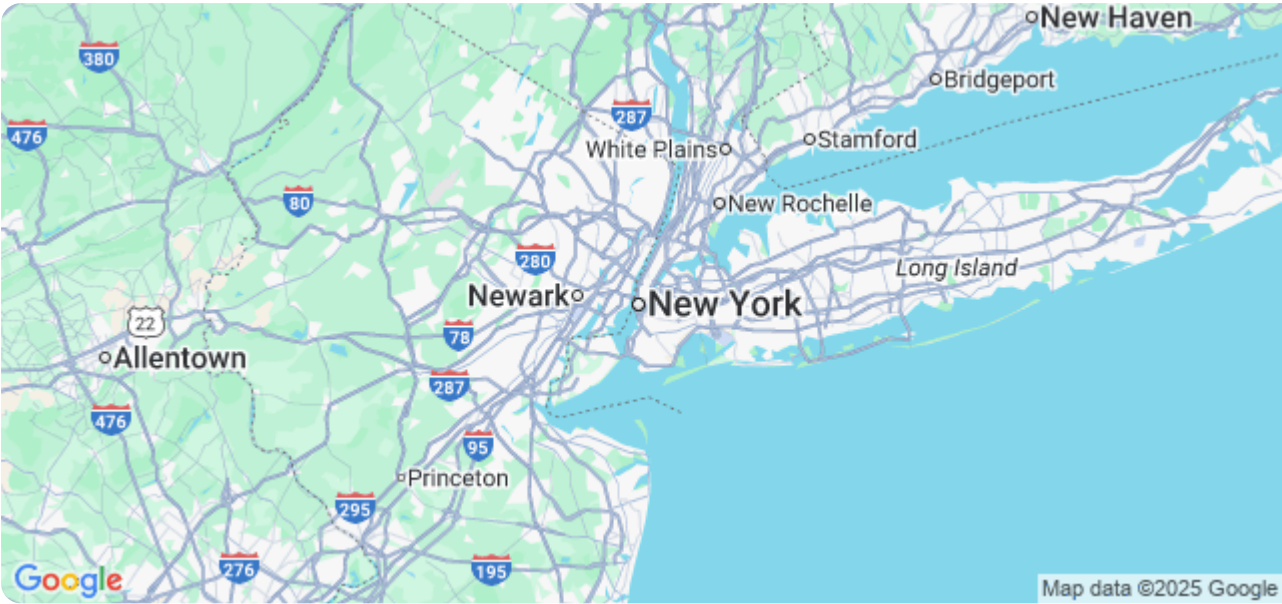
Time Breach Detected

Initial Description of Suspected Breach

Write something...

Geographic Location of Initial Detection (if applicable)

📍 Set My Current Location



Initial Suspected Cause (e.g., Malware, Phishing, Insider)

- ☐ Malware
- ☐ Phishing
- ☐ Insider Threat
- ☐ System Vulnerability
- ☐ Unknown

Estimated Number of Records Potentially Affected

Enter a number...

Upload Initial Log Files/Screenshots (if available)

 Upload File

Actions Taken to Immediately Contain the Breach (e.g., System Isolation)

Write something...

Legal & Regulatory Notification

Determining notification requirements and initiating communication with relevant authorities.

Date Breach Discovered

Enter date...

Applicable State Notification Laws

- ☐ No State Laws Apply
- ☐ California AB 205
- ☐ New York SHIELD Act
- ☐ Other (Specify)

Summary of Breach Details for Regulatory Reporting

Write something...

Federal Notification Required (HIPAA)?

- ☐ Yes
- ☐ No

Estimated Number of Individuals Affected (Federal)

Enter a number...

Date of First Regulatory Notification Sent

Enter date...

Summary of Notifications Sent to Federal Regulators (e.g., HHS)

Write something...

Patient Notification & Communication

Preparing and delivering notifications to affected patients.

Draft Patient Notification Letter

Write something...

Notification Method(s)

- ☐ Postal Mail
- ☐ Email
- ☐ Phone Call
- ☐ Website Announcement

Date of Initial Patient Notification

Enter date...

Number of Patients Notified (Estimated)

Enter a number...

Script for Phone Call Notifications (if applicable)

Write something...

Copy of Website Announcement (if applicable)

 Upload File

Designated Contact Person for Patient Inquiries

Vendor Notification & Management

Informing and collaborating with third-party vendors involved.

Vendor Notification Status

- ☐ Notified
- ☐ Notification Pending
- ☐ Notification Complete

Vendor Contact Details

Write something...

Vendor Representative Name

Write something...

Vendor Case/Incident Number (if applicable)

Enter a number...

Date of Vendor Notification

Enter date...

Summary of Vendor Response/Actions

Write something...

Vendor Support Level

- ☐ Full Support
- ☐ Limited Support
- ☐ No Support

Forensic Investigation

Engaging experts to investigate the root cause and gather evidence.

Initial Breach Narrative

Write something...

Estimated Records Potentially Accessed

Enter a number...

System Logs (Relevant Timeframe)

 Upload File

Attack Vector Identified (e.g., Phishing, Malware)

- ☐ Phishing
- ☐ Malware
- ☐ Insider Threat
- ☐ Vulnerability Exploit
- ☐ Unknown

Date of Initial Intrusion (Estimated)

Enter date...

Time of Initial Intrusion (Estimated)

Description of Forensic Tools Used

Write something...

Remediation & Security Enhancements

Implementing measures to prevent future breaches and improve security posture.

Number of Vulnerabilities Patched

Enter a number...

Security Controls Implemented (Select all that apply)

- ☐ Enhanced Firewall Rules
- ☐ Multi-Factor Authentication
- ☐ Data Encryption (at rest & in transit)
- ☐ Intrusion Detection/Prevention System Updates
- ☐ Endpoint Detection and Response (EDR) Deployment
- ☐ Security Awareness Training (Reinforcement)

Detailed Description of Remediation Steps

Write something...


Date of Final Patch Deployment

Enter date...

Vulnerability Scanning Frequency

- ☐ Weekly
- ☐ Bi-Weekly
- ☐ Monthly
- ☐ Quarterly

Proof of Patch Application (Screenshot/Log)

 Upload File

Documentation & Reporting

Maintaining a comprehensive record of the breach response activities.

Detailed Breach Timeline

Write something...

Estimated Number of Records Affected

Enter a number...

Forensic Investigation Report

 Upload File

Summary of Remediation Actions Taken

Write something...

Date of Initial Breach Detection

Enter date...

Time of Initial Breach Detection

Communication Records with Legal Counsel

Write something...

Post-Breach Review & Evaluation

Analyzing the response and identifying areas for improvement.

Estimated Total Cost of Breach (USD)

Enter a number...

Effectiveness of Communication Plan

- ☐ Highly Effective
- ☐ Moderately Effective
- ☐ Somewhat Effective
- ☐ Not Effective

Lessons Learned and Recommendations

Write something...

Date of Next Security Audit

Enter date...

Areas for Security Enhancement (Select All That Apply)

- ☐ Employee Training
- ☐ System Access Controls
- ☐ Data Encryption
- ☐ Incident Response Plan
- ☐ Vendor Management

Name of Reviewer

Write something...

Date of Review Completion

Enter date...