

****<Organization Logo>****

Security Incident Response Plan

<Date>

Table of Contents

[Revision History 3](#_Toc141354978)

[1 Overview 4](#_Toc141354979)

[2 Preparation 7](#_Toc141354980)

[3 Detection & Analysis 15](#_Toc141354981)

[4 Security Incident Containment, Eradication, & Recovery 21](#_Toc141354982)

[5 Post Incident Activity 23](#_Toc141354983)

[6 References 26](#_Toc141354984)

[Appendix A: *SAMPLE* Security Incident Response Checklist 27](#_Toc141354985)

[Appendix B: Communications 29](#_Toc141354986)

[Appendix C: Security Incident Response: Lessons Learned Evaluation Form 36](#_Toc141354987)

[Appendix D: Security Incident Play Books 38](#_Toc141354988)

[Appendix E: Example Containment Strategy 39](#_Toc141354989)

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description of Change |
| 0.01 | 8/30/2020  |  | Initial draft Template Design  |
| 0.02 | 12/16/2020 | Shelby Kobes |  |
| 0.03 | 3/20/2023 | M.Erikson | Revise to new format |
| 0.4 | 7/26/2023 | M.EriksonR. Mastin  | * Updated to align with recently released Healthcare & Public Health Sector Coordinating Councils [Coordinated Healthcare Incident Response Plan (CHIRP)](https://healthsectorcouncil.org/wp-content/uploads/2023/07/HIC-CHIRP-FINAL_1.pdf) template. Includes adding a sample Containment Strategy (as Appendix E)
* Enhanced role of Cyber-Liability Plan Insurer
 |

# Overview

|  |
| --- |
| * TEMPLATE INSTRUCTIONS AND NOTES (DELETE BEFORE PUBLISHING)
* Text in red is highlighted for Organization-specific updates
* HR 7898, HIPAA Safe Harbor Bill, amended the HITECH Act to direct HHS to provide regulatory relief and considerations for HIPAA covered entities which have met Recognized Cybersecurity Practices, such as NIST and 405d. To support organizations in the implementation of Recognized Cybersecurity Practices, this Plan template has been developed largely from NIST standards. Where appropriate, other industry standards and best practices have been incorporated.
* Don’t forget to Print this plan and any supporting documents and give a copy to everyone you expect to play a role in an incident. During an incident, your internal email, chat, and document storage services may be down or inaccessible.
* This plan is designed to interact with and coordinate activities from various other organizational plans including Cybersecurity Playbooks, Disaster Recovery Plans, Hospital Incident Command Procedures, Business Continuity Plans, Emergency Management Plans, and Downtime Procedures.
* Disruptive events not arising from a cyberattack are considered out of scope for this plan and should be managed according to the appropriate subject area plans. Additionally, cyber related events that do not rise to the disruptive incident classification are out of scope for this plan and should be managed according to the appropriate Plan and/or Playbooks.
 |

Security incident response is an organized approach to addressing and managing activities during and after a suspected IT security event. The goal of security incident response is to handle the situation in an organized and effective manner that limits damage to the organization and reduces recovery time and cost. This Security Incident Response Plan provides guidelines on what constitutes an incident, along with a process that must be followed when a security incident occurs.

This Plan aligns with *National Institute for Standards and Technology (NIST) Special Publication 800-61: Computer Security Incident Handling Guide v2,* and other industry standards and best practices. *NIST 800-61 v2* recognizes four key phases for the security handling lifecycle:



***NIST 800-61: Computer Security Incident Handling Guide Phases***

Thorough incident response process includes identifying an attack, understanding its severity, deploying mitigating actions, restoring operations, and implementing appropriate actions to help prevent its reoccurrence in the future. The arrows in the diagram are important as NIST emphasizes that incident response is not a linear, but rather a cyclical activity, with an emphasis on continuing learning and improvement to further strengthen an organization’s defense against increasing security threats.

## Purpose

The purpose of this Plan is to provide a set of documented procedures, guidelines, and protocols detailing the steps that should be taken in each phase of incident response to ultimately protect information assets from security threats and maintain the confidentiality, integrity, and availability of information systems.

Details included in the Plan address two key security threats:

* **Event** –  which NIST defines as “any observable occurrence in a network or system.”
* **Incident** – which NIST defines as “an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.”

The goal is to properly identify, triage, and mitigate security events before they become an incident.

## Policy Statements

This Plan is supported by <Security Incident Response Policy or insert relevant Organizational policy> which governs procedures, roles, and responsibilities outlined throughout this Plan.

## Compliance

The Organization will employ multiple methods, tools, and audit processes to monitor and assess whether security controls and measures have been implemented and are being followed.

Non-compliance with this Plan will result in notifications to the employee and management. Further consequences may include disciplinary action up to and including termination of employment and/or legal proceedings to recover any loss or damage to the Organization, and possibly third parties affected. Additional details on Compliance and Exceptions are outlined in the supporting Policy.

## Confidentiality

All security events are considered confidential. Best effort shall be made to maintain the confidentiality of employees reporting security events.

All evidence and artifacts discovered, captured, or generated during the incident response by the Organization and those working in conjunction with the Organization responding to the security incident are considered confidential and only shared with those who have a business need which is approved by the <insert Role>.

All email communication regarding the security incident shall be marked as privileged.

## Plan Organization and Content

The Security Incident Response Plan includes recommended procedures and processes to support an end-to-end response to a suspected or identified security incident. Processes align with the four phases as outlined above. A consolidated list of recommended activities is included in Appendix A: Sample Security Incident Response Checklists.

Additional supporting forms referenced throughout this Plan are provided as separate attachments.

# Preparation

|  |
| --- |
| TEMPLATE INSTRUCTIONS AND NOTES (DELETE BEFORE PUBLISHING)* *NIST 800-61 v2* reflects three primary models for security incident response team (SIRT) organization. This Plan was developed off a Central SIRT.
	+ Central—*centralized body that handles incident response for the entire organization.*
	+ Distributed—*multiple incident response teams, with each one responsible for a physical location (e.g. branch office), a department or a part of the IT infrastructure*
	+ Coordinated—*a central incident response team that works together with distributed incident response teams, without having authority over them. The central team serves as a knowledge center and offers assistance with complex, critical, or organization-wide incidents.*

Per *NIST 800-61 v2*, Organizations who are determining their IRT model and staffing should consider the following: * + - Does incident response need to be available 24/7? *24/7 may be costly and not always be required for certain organizations and operating models.*
		- Do incident responders need to be on-site or is phone contact sufficient? *Real-time availability and on-site presence is best because it allows immediate response to an incident, which can prevent damage.*
		- Should staff be part-time or full-time? *Part-time employees can be used to make up a virtual incident response team. When an incident occurs, the IT help desk often serves as the first point of contact.*
		- What level of expertise is needed? *Incident response requires broad range of knowledge. Outsourced teams typically have stronger security expertise, but employees have a better understanding of the Organization’s environment and culture.*
* The roster for the SIRT Team should be established with considerations both to appropriate organizational authority and appropriate subject matter expertise to raise and evaluate the risks and tradeoffs of potential decisions and courses of action.
* For Tables 2-1 through 2-4, insert appropriate roles and contact information. In some cases, a single person may be responsible for multiple roles.
* Some additional best practices to consider in this Preparation Phase:
	+ Consider including secondary contact information for the SIRT in cases where communication is severely limited. Identify additional/supplemental staff to provide backup to primary members that may not be able to fulfill their duties due to other responsibilities, or extenuating circumstances (e.g., illness).
	+ Ensure teams are comprised of representatives from all functional areas of the organization system, including clinical, non-clinical, support, and ancillary departments.
	+ For more information on contingency planning as it relates to cybersecurity, the [*NIST SP 800-34 v1: Contingency Planning for Federal Information Systems*](https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final)document provides specific information on the purpose, process, and format for formal contingency planning within the IT sector.
 |

Preparation activities work to both establish incident response capability so that the Organization is ready to respond to incidents, while also preventing incidents through controls like staff awareness and vulnerability monitoring. This section includes ongoing preparation activities to support security incident response.

## Roles and Responsibilities

### Security Incident Response Team (SIRT)

The <Security Incident Response Team (SIRT) or insert alternative name for team> consists of the following primary and alternate members:

**Table 2-1: SIRT Member Contact List**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Core SIRT Member Title** | **Name and Primary Contact** | **Secondary Contact** | **Backup**  |
| 1 | Incident Response Manager / CISO |  |  |  |
| 2 | Technology Manager |  |  |  |
| 3 | Communications Manager |  |  |  |
| 4 | Internal Support Services (ISS) |  |  |  |
| 5 | Hosting Service Desk (HSD) |  |  |  |
| 6 | Server and Desktop Support Services |  |  |  |
| 7 | Network Support Services |  |  |  |
| 8 | EMR Services Lead |  |  |  |
| 9 | Hosting Services Urgent Process Response Team |  |  |  |
| 10 | <Other> |  |  |  |

The Extended Security Incident Response Team (Extended SIRT), depending on the circumstances and type of security incident, may include the following members.

**Table 2-2: Extended SIRT Member Contact List**

| **No.** | **Extended SIRT Member Title** | **Name and Contact** |
| --- | --- | --- |
| 1 | Legal Department / Information Privacy Office |  |
| 2 | Human Resources |  |
| 3 | Workplace Services |  |
| 4 | Corporate Communications / Public Relations |  |
| 5 | Building Management  |  |
| 6 | Cyber Liability Provider\*  |  |
| 6 | Other\* – *Note: If external agencies or organizations are required to be notified of incidents, they should be added to table above (IR partners, FBI, Cyber Insurance … etc).* |  |

\*Depending on your cyber liability plan and requirements

### Roles and Responsibilities

The SIRT's role is to provide a quick, organized, and effective response to security related events. The SIRT’s mission is to prevent a serious loss of information, information assets, property, and customer confidence by providing an immediate, effective, and informed response to any event involving information systems, networks, or workplace.

The SIRT is authorized to take appropriate steps necessary to contain, mitigate, and resolve a security incident. The team is responsible for investigating suspected intrusion attempts, reporting and loss of company information and assets in a timely manner.

Team members must be able reprioritize their daily responsibilities to respond to a security incident and must have the appropriate level of authority to make decisions regarding risk and security measures.

Below are roles and responsibilities of the SIRT Team:

**Table 2-3: SIRT Member Responsibilities**

| **Functional Role** | **Description / Responsibilities** |
| --- | --- |
| Incident Response Manager / CISO | * Determines the nature and scope of the security incident
* Contact insurances and security consultants
* Contacts the SIRT members
* Determines resources necessary to aid in security incident response
* Coordinates security incident response efforts
* Escalates to management as appropriate
* Contacts other departments as appropriate
* Monitors and reports on the progress of the investigation to <insert appropriate departments and agencies>
* Ensures evidence gathering, chain of custody and preservation is performed as appropriate
* Prepares a written summary of the security incident and corrective actions taken
* Organizes and participates in Lessons Learned meetings
 |
| Technology Manager | * Serve as the Technical subject matter expert.
* Coordinate internal and possibly external technical experts as appropriate for the response
* Notifies Workplace Services of physical security breaches
* Escalates incidents as necessary
 |
| Communications Manager | * Manage communications both internally and externally in accordance with the approved Communications Plan
* Prepares appropriate response to media, customers and/or employees, and coordinates with Legal and Privacy Office for approval prior to distribution
* Coordinates with Legal Department / Information Privacy Office on timing, content and method of notifications
* Prepares and issues press release statement if necessary
* Monitors media coverage and distributes as needed
 |
| Service Desk  | * Receives incident notifications from stakeholders
* Monitors the environment
* Reports security incidents to ISS or the CISO
 |
| Server and Desktop Support Services | * Performs containment, eradication and remediation tasks based on CISO guidance
* Installs service packs and patches
* Installs malware abatement software
* Ensures that backups are in place for all critical systems
* Ensures that system logs are available and assists the CISO in analysis / investigations
 |
| Network Support Services | * Performs analysis, containment and remediation tasks based on CISO guidance:
* Analyzes network traffic
* Runs tracing and monitoring tools such as sniffers, port monitors, traffic analyzers, etc.
* Takes actions necessary to block traffic from suspected sources
* Investigates signs of firewall breach
* Contacts Internet Service Providers
 |
| EMR Service Lead/ Hosting Services Urgent Process Response Team | * Activates <Urgent Process Response Team for Hosting Operations or other hosting team name> based on CISO guidance
* Performs containment, eradication, and remediation tasks on Hosting Operations infrastructure
* Handles communications with Hosting Clients and EMR Systems
* Escalates issues to the CISO
 |

Below are roles and responsibilities of the Extended SIRT:

**Table 2-4: Extended SIRT Member Responsibilities**

| **Functional Role** | **Description / Responsibilities** |
| --- | --- |
| Legal Department/ Information Privacy Office | * Coordinates activities with the CISO
* Identifies and documents the types of PII/PHI that may have been breached
* Provides guidance throughout the investigation on issues relating to the privacy of customer and employee data
* Assesses the need to update privacy policies, procedures, and practices as a result of the security incident
* Provides guidance to the CISO on legal matters such as evidence collection, the need for computer forensics, legality and the liabilities of certain actions
 |
| Risk Management Office | * Coordinates activities with the CISO
* Assists in determining the overall impact to the organization
* Performs risk analysis as required
* Delivers appropriate communications to impacted parties
* Assesses the need to change risk management policies, procedures, and practices as a result of a security incident
 |
| Human Resources | * Handles issues relating to employees such as interviews on sensitive matters, disciplinary actions, etc.
* Provides guidance to the CISO on matters relating to Human Resources
 |
| Workplace Services | * Coordinates activities with CISO
* Assists in providing video footage and proximity card transactions to CISO for investigation
* Contacts law enforcement for physical security breaches
 |
| Cyber-Liability Plan Insurer\*  | * Advises on plan requirements or guidelines to ensure actions align with cyber-liability coverage.
 |

### RASCI Matrix

The Responsibility Assignment Matrix (RASCI) describes the level of participation by various roles in handling different stages of the incident response lifecycle. The RASCI matrix is comprised of the following actions:

**R – Responsible** – owns the action; is responsible for completion

**A – Accountable** – ultimately accountable for completion

 **S – Supporting** – provides resources or plays supporting role

**C – Consulted** – provides information or has capabilities to necessary to complete work

**I – Informed** – must be notified of results, but does not need to be consulted

**Table 2-5: RASCI**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Users** | **Incident Response Manager** | **Technology Manager** | **Comm Manager** | **Server / Desktop Support** | **Network Services** | **Urgent Response Team** | **Legal / IPO** | **HR** | **Workplace Services** | **RMO** | **Cyber-Liability Plan** |
| **Detection** | R | R | R | S | R | R | R | I | I | R | I | I |
| **Notification** | I | R | I | R | I | I | I | I | I | I | I | I |
| **Analysis** | C | R | S | S | C | C | C | C | I | C | I | I |
| **Containment** | I | R | R | I | C | C | C | I | I | I | I | I |
| **Eradication** | I | R | R | I | C | C | C | I | I | I | I | I |
| **Recovery** | I | R | R | I | S | S | S | C | I | I | C | I |

## Critical IT Assets

The Organization has determined critical IT assets in accordance with the <Asset and Data Management Policy or insert other applicable policy>. A current inventory of IT assets can be found <insert location>. The IT Asset inventory may be used to support analysis and recovery of identified incidents.

## Staff Training

All staff need to understand their role in maintaining and improving the security of the organization. That includes knowing how to identify and report suspicious events. Security Incident Response are integrated into the Organization’s security awareness training program in accordance with the <Security Awareness and Training Policy or insert other applicable policy> and include updated training to communicate changes to this Plan or any supporting procedure.

The organization also sends periodic reminders by:

* <Sending reminder emails about security threats>
* <Sharing stories and news articles of organizations that have experienced cyber attacks>
* <Placing cybersecurity printed materials around facilities>
* <Providing periodic cybersecurity reminders and discussion topics at board and management meetings>
* <Other>

To help inform periodic updates and awareness of new and rising threats, the Organization receives up-to-date alerts and guidance from the following federal sites and partners:

* <Health Sector Cybersecurity Coordination Center (HC3): [Products](https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#sector-alerts)>
* <HHS Healthcare and Public Health Sector: [Highlights-Cybersecurity Edition](https://www.phe.gov/Preparedness/planning/cip/Pages/CIPInquiry.aspx)>
* <HHS 405(d): [Subscribe to The Post](https://405d.hhs.gov/)>
* <CISA: National Cyber Awareness System Bulletins/Reports; [Sign-up for Alerts](https://www.cisa.gov/uscert/ncas)>
* <CISA: [SHIELDS UP webpage](https://www.cisa.gov/shields-up)>
* <CISA: [Stop Ransomware webpage](https://www.cisa.gov/stopransomware)>

## Incident Response Plan Testing

|  |
| --- |
| TEMPLATE INSTRUCTIONS AND NOTES (DELETE BEFORE PUBLISHING)* Organizations may consult the following free resources when planning their Tabletops:
	+ CISA Tabletop Exercise Packages: <https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages>
	+ Department of Homeland Security Cyber Tabletop Exercise for Healthcare Industry: <https://cdn.ymaws.com/ahepp.site-ym.com/resource/resmgr/HSEEP/Healthcare_Cyber_TTX_Facilit.doc>
 |

This Security Incident Response Plan will be tested periodically to ensure that Workforce Members involved are aware of their roles and responsibilities, and that the content of the plan is valid in the current environment.

### Testing Requirements

The Organization will perform a Tabletop exercise that tests higher risk security incidents at least once <annually or insert alternative timeframe> in accordance with the <Security Incident Response Policy or insert appropriate policy name>. Tabletop exercises are discussion-based group tests used to validate (and update as necessary) the processes, roles, and responsibilities included in this Plan to ensure effective response to different types of security incidents are in place.

Each table-top exercises will run through various layers of security incidents that will:

* Ensure that all organizational and process flow charts are up to date with current department and group alignments;
* Ensure that all personnel involved with the IRP are aware of their roles and responsibilities with each type of security incident;
* Ensure that the security incidents incorporate some form of group problem-solving strategy;
* Examine contingencies, dependencies, and inter-department coordination needs.

### Testing Documentation and Results

Results from Tabletop exercises should be documented and incorporated as revisions to this Plan. The Tabletop exercise may also result in other Action Plans or identified risks, which will be incorporated into the Organization’s Risk Management framework. Revisions to this Plan should are reflected in the Revision History.

## Other Preparation Tasks

To sufficiently prepare for security incidents, the Organization will conduct periodic activities to optimize its security incident response program:

* **<Review the Plan with Legal** for insight into how to engage with outside incident response vendors, law enforcement, and other stakeholders.>
* **<Meet the CISA regional team**, including local and regional Protective Security Advisors (PSAs), Cybersecurity Advisors (CSAs), Emergency Communications Division Coordinators, and other CISA personnel to handle a wide array of needs.>
* **<Meet local law enforcement agency (LEA) team** in coordination with Legal, to review local threats and communication processes.>
* <**Meet with vendors** to coordinate on security incident response coordination and detection.>
* **<Routinely print up-to-date user lists**to allow for quick identification of malicious accounts and rapid recovery in the event systems are down.>
* **<Review IRP plan annually** or after a response to any cybersecurity incidents or material changes to organizational structures or associated detailed plans**>**

# Detection & Analysis

|  |
| --- |
| TEMPLATE INSTRUCTIONS AND NOTES (DELETE BEFORE PUBLISHING)* The Security Intake Form is provided as an attachment to this Plan as an example. Ideally, incidents are recorded in some type of software or ticketing system for more robust reporting and analysis.
* For Tables 3-2 and 3-6, update with the Organization’s specific definitions.
* 3.2.1 reflects an email-based notification process. Organizations with systems or other processes should revise as necessary.
 |

Detection can happen from many venues – including IT monitoring systems and security tools, publicly available information, and most often, from people inside and outside the organization.

Proper analysis allows the Organization to review the security event, analyze it against a baseline of normal activity for the affected systems, correlate related events, and systematically categorize incidents to effectively triage it for containment.

## Identification

Users of information services are required to note and report any observed or suspected security weaknesses in, or threats to, systems or services. Users will report these matters to their management or as detailed in this Plan.

Users will be informed that they should not, in any circumstances, attempt to prove a suspected weakness. This is for their own protection, as testing weaknesses might be interpreted as a potential misuse of the system.

All Workforce Members will be made aware of the procedure for reporting security incidents and will be required to report such incidents as quickly as possible. Suitable feedback processes will be implemented to ensure that those reporting incidents are notified of results after the incident has been dealt with and closed.

### Security Incident Intake Process

The <Helpdesk or insert other role or group> will serve as the central point of contact for reporting any security event or confirmed security incidents.

The table below outlines actions the <CISO and SIRT or insert other roles> must take to record, triage, and document the report.

**Table 3-1: Security Reporting Procedure**

| **Step** | **Actions** |
| --- | --- |
| 1 | User calls the <Helpdesk, CISO, or insert role>**OR**User calls <**1-XXX-XXXXXXX>** to report a potential event. |
| 2 | The analyst record details of the potential event using the <***Security******Incident Intake Form*** or insert other mechanism for recording.> SIRT personnel are responsible for asking questions about an event, making reasonable attempts at determining if an incident has occurred, and recording facts and responses to questions. Some of the questions the analyst should ask to determine whether an incident has occurred are:* How was the incident discovered?
* Describe the evidence that substantiates or corroborates the incident (e.g., eyewitness, video footage, screen-shots, hard copy, etc.)
* Identify all parties with knowledge of the incident
* Provide details on nature of the data involved in the incident
* How the information was held? Identify the types of information systems and/or the media on which the information was stored (e.g., hardcopy, laptop, flash drive, etc.).
* Who currently holds any evidence from the incident?
 |
| 3 | The analyst must inform the individual to expect to be contacted by a member of the SIRT. |
| 4 | The analyst must request that the individual treat the incident a confidential matter and stress this should not be communicated further without proper consent. |
| 5 | The analyst will perform or assist in triaging the incident using available resources such as <Desktop Support, Server Support or Network Support or insert other role.> |
| 6 | The analyst will assign an initial priority rating based on the details of the incident. |

### Security Incident Prioritization

The analyst will assign an initial prioritization based on the following definitions:

**Table 3-2: Incident Prioritization Matrix**

| Priority | Definition | Examples |
| --- | --- | --- |
| **Urgent** | An incident that severely affects multiple systems, organizations or mission critical infrastructure, and results in significant loss of confidentiality, integrity and availability of information along with the loss of ePHI.  | Examples of Urgent priority security incidents are:* Successful system break-in (hacking)
* Attacks against critical infrastructure, network, or production systems
* Confirmed breaches of PII/PHI/ePHI
* Confirmed violations of policy
* Confirmed malware epidemic
* Ransomware
* Confirmed discovery of unauthorized software such as Trojans, backdoors, rootkits, and Ransomware, on the network
* Complete unavailability of mission critical resources due to a security threat
 |
| **High** | An incident that moderately affects multiple systems, organizations or critical infrastructure that is not mission- critical, and results in some loss of confidentiality, integrity, and availability of information. | Examples of High priority security incidents are:* Suspected breach of PII/PHI/ePHI
* Unauthorized access to critical system(s)
* Loss or theft of property containing proprietary or confidential information
* Detected network scans from unauthorized sources
* Suspected violations of policy by employees, contractors, or other third-parties
* Confirmed malware detection or Phishing activities
 |
| **Medium** | An incident that moderately affects a single system, organization or infrastructure that is not mission critical OR an incident with negligible impact on multiple systems, organizations or non-critical infrastructure. | Examples of Medium priority security incidents are:* Sharing of passwords or accounts
* Loss or theft of property regardless of value of information
* Suspected malware presence
 |
| **Low** | An incident with minimal or negligible impact to the system(s), organization(s) or infrastructure, and does not result in any loss of confidentiality, integrity or availability of information. | Examples of Low priority security incidents:* Unintentional actions by user (e.g., multiple login failures due to user error or automation)
* Unintentional damage or loss of recoverable information
* Attempted access to unauthorized websites
 |

## Incident Triage

### Notification of Incident

The table below outlines actions that <SIRT analysts or insert specific role> must take to notify the <CISO or insert role> on-call staff:

**Table 3-3: Incident Notification Procedure**

| **Step** | **Actions** |
| --- | --- |
| **For All Security Incidents** |
|  | Notify the <CISO> by sending an e-mail to: <Email> This e-mail will be received by all <CISO> team members and will also page the <CISO> staff on-call.* The e-mail subject line should have the following format:

“Security Incident Reported – Incident:[Incident Number] - [Initial Impact Rating] – [Initial Type of Incident as determined by the analyst].Notifications should be sent to the <CISO> in accordance with the following Service Level Agreement timelines:

|  |  |
| --- | --- |
| **Initial Priority Rating** | **Maximum Time To Contact the CISO**  |
| Urgent | <5 minutes> |
| High | <15 minutes> |
| Medium | <1 hour during regular business hours> |
| Low | <2 hours during regular business hours> |

  |
|  | Save the <Security Incident Intake form> to the <Secure SharePoint location> for the <CISO> to retrieve it.The file name should have the following format: “Security Incident [Incident Number]” |
|  | Open a tracking ticket to <insert system or tool used for internal tracking>. This will be used for tracking purposes. |
|  | The <insert Role> enacts the Communication Plan and works with <insert group> to distribute appropriate notifications. |
| **For Physical Security Incidents** |
|  | Follow notification procedure steps 1-3.  |
|  | Call the appropriate <Workplace Services or other role> phone numbers. A list of <Workplace Services or other role> contacts is included in Table 2-1. |
|  | The <insert Role> enacts the Communication Plan and works with <insert group> to distribute appropriate notifications. |
| **For Suspected Breaches of ePHI/PHI** |
|  | Follow notification procedure steps 1-3. |
|  | The <CISO> coordinates with <Legal, Privacy Officer or insert other roles> to conduct a Breach risk assessment to determine if an impermissible use or Disclosure of PHI constitutes a Breach of Unsecured PHI and whether individuals, media, or the HHS secretary must be notified. The Breach risk assessment must include:* The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
* The unauthorized person who used the PHI or to the Disclosure was made;
* Whether the PHI was actually acquired or viewed; and
* The extent to which the risk to the PHI has been mitigated.

If a risk assessment is not completed, the Organization must presume the impermissible use or Disclosure of PHI rises to the level of a Breach of Unsecured PHI and is required to send notification(s), as outlined below. |
|  | Document the Breach risk assessment and investigation, including any outcomes in the <Security Breach Tracking Form or other mechanism>. |
|  | The <insert Role> enacts the Communication Plan and works with <insert group> to distribute appropriate notifications.  |

### Security Incident Escalation Procedures

For incidents reported to the <CISO>, the staff on-call should acknowledge the receipt of incident notification as soon as it is received, or at a minimum adhere to the following SLA timelines for acknowledging the incident following notification:

**Table 3-4: Incident Acknowledgement Timeframes**

| **Priority Rating** | **Time to acknowledge the notification of security incident** |
| --- | --- |
| Urgent | <10 minutes> |
| High | <20 minutes> |
| Medium | <2 hours during regular business hours> |
| Low | <24 hours during regular business hours> |

<SIRT or insert role> should follow the escalation timeframes below service level response times are not met. This will help management to optimize resource allocations so that a resolution can be achieved in the specified timeframes.

**Table 3-5: Incident Escalation Timeframes**

|  |  |
| --- | --- |
| **Priority Rating** | **Escalate to the SIRT by e-mail if the CISO does not respond within:** |
| Urgent | <15 minutes> |
| High | <30 minutes> |
| Medium | <2 hour during regular business hours> |
| Low  | <12 hours or by next business day> |

## Incident Analysis

The <CISO> is responsible for performing detailed analysis of a reported or discovered security incident based on available information and by utilizing all available tools to determine the impact, priority, and severity of the incident. The <SIRT> may change the initial priority rating of the incident based on the results of their analysis. All confirmed Urgent, High, and Medium priority incidents must be documented by the <CISO>.

### Security Incident Severity Rating

During the analysis and after confirmation that a security incident has occurred, the <CISO> must assign the severity rating to the incident in accordance with the following definitions:

**Table 3-6: Incident Severity Ratings**

| Severity | Definition |
| --- | --- |
| **Severity 1** | A security incident that requires multiple resources to contain/eradicate and resolve. Multiple SIRT members involved. The SIRT must meet all SLAs.**Any confirmed breach of** **PII/PHI/ePHI.** |
| **Severity 2** | A security incident that requires timely attention but can be contained/eradicated and resolved by the <CISO> with minimal support from the SIRT and external resources. |
| **Severity 3** | A security incident that can be quickly contained/eradicated and resolved by the <CISO> without support from the SIRT or external resources. |

After assignment of the severity, the <CISO> should enact the Triage procedure.

**Table 3-7: Incident Triage Procedure**

| **Step** | **Action** |
| --- | --- |
| 1 | Obtain a room and/or establish conference call bridge. |
| 2 | Page or call appropriate primary and secondary SIRT members to join an incident response meeting:* For **Urgent/High** priority, within <30 minutes or insert timeframe>
* For **Medium/Low** priority, within <4 hours or or insert timeframe>
 |
| 3 | Conduct an initial incident response meeting to inform the SIRT of the nature of the incident and determine the containment, eradication, and recovery strategy. |
| 4 | Schedule follow-up meetings based on the priority of the incident:* For **Urgent/High** priority, send updates every <2 hours or insert timeframe> and hold meetings as necessary until the incident is resolved.
* For **Medium/Low** priority, send daily updates and hold meetings as necessary until the incident is resolved
 |
| 5 | Mandatory Key External or Extended contacts should be notified and provided status updates when required/applicable |

# Security Incident Containment, Eradication, & Recovery

|  |
| --- |
| TEMPLATE INSTRUCTIONS AND NOTES (DELETE BEFORE PUBLISHING)* Typically, activities in this section are supported by a Business Continuity and Disaster Recovery Plan, which should also include data backup and restoration procedures. That should be referenced as appropriate.
* To support restoration, the organization should regularly test backup RTO and RPO objectives. It is difficult to test full system restores from backups because of disruption to patient services
* Each Organization should know its thresholds for what triggers a system shutdown.
* We recommend organizations include specific playbooks to common scenarios as attachments to help guide this phase.
 |

Once an incident has been verified by the SIRT, it is vital to contain the incident as soon as possible to limit the potential impact. The SIRT should plan its containment procedures and strategies so to help coordinate its actions and increase responsiveness during a confirmed incident. Close communications should be coordinated with stakeholders in accordance with the approved Communication Plan.

Containment procedures vary greatly depending on the type of incident and are highlighted in this Plan. There are often several strategies to choose from, so the SIRT should ask the following questions to determine the best method of containment:

* What is the potential impact to affected resources?
* How important is the preservation of evidence?
* Is it necessary to maintain network and service availability? (e.g., network connectivity, services to partners or external parties)
* How much time and effort will be needed to implement the containment strategy?
* How effective is the containment strategy? Does it partially or fully contain the incident?
* How long will the strategy be effective? Is it temporary or permanent?
* Is extortion involved? Do we have an extortion plan we can refer to?
* Can we continue business according to a Business Continuity Plan?
* Can resources from paused operations be reallocated to support downtime procedures?

**An example Containment Strategy is included in Appendix E.**

After an incident has been contained, the SIRT should begin eradication and recovery procedures. In terms of response, it is important to differentiate between eradication of the threat actor and restoration of services as both are critical steps. Intrusions could restore services without removing the threat, resulting in either an on-going cycle of compromise, or having a dormant threat remaining on the network.

These two stages often include overlapping actions, as they both involve returning systems to their normal states. The following steps should be considered during eradication and recovery:

* Prevent attackers from launching the same exact attack (e.g., delete malicious code, disable breached accounts)
* Leverage external stakeholders as needed to inform the response effort.
* Remove artifacts left over by the incident (e.g., extraneous files)
* Restore systems using clean backups or build images
* Handle data backload caused by downtime.
* Begin media relation activities (if applicable)
* Plan for migration of manual documentation back to electronic format once systems are restored.
* Increase security across the entire organization to prevent similar attacks from exploiting the same vulnerabilities. For example:
	+ Increase password complexity requirements
	+ Update firewall rules and router access control lists
	+ Implement processes for vulnerability scanning across all systems
	+ Implement processes for installing patches across all systems
	+ Reconfigure monitoring tools to detect specific anomalies in network and system usage

Containment strategies may be lifted once the incident has been confirmed as eradicated and technical recovery has been validated. Criteria for declaring the incident is closed and operations are returned to normal shall be captured in the <Security Incident Response Form or other appropriate mechanism>. Stakeholders will be notified in accordance with the approved Communications Plan.

# Post Incident Activity

|  |
| --- |
| TEMPLATE INSTRUCTIONS AND NOTES (DELETE BEFORE PUBLISHING)* In some cases, organizations align incident response with general emergency management procedures. Some organizations may leverage the FEMA-based After Action Report/Improvement Plan. A sample template can be found [here](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjI_PjnjPD9AhX6JDQIHR1TDjUQFnoECA8QAQ&url=https%3A%2F%2Ftraining.fema.gov%2Fhiedu%2Fregionalengagement%2F_assets%2Fregion_v_report_final_collaborative_engagement.docx&usg=AOvVaw0DntLkXD1Gh3wU4TaWpVcZ).
 |

A central part of the NIST incident response methodology is learning from previous incidents to improve the process.

## Root Cause Analysis

Root cause analysis is a process designed for use in investigating underlying causes of events that led to or were directly responsible for the security incident. It aims to identify not only what happened and how it happened, but most importantly, why it happened. Only when investigators are able to determine why an incident occurred, it is possible to implement workable corrective measures that prevent similar future events from occurring.

In root cause analysis it is important to understand that:

* Root causes are specific underlying causes. The goal should be to identify specific causes of why incident occurred which will lead to more realistic and implementable recommendations. General cause classifications such as "equipment failure" or "external factors" should not be used since the classifications are not specific enough for implementing effective changes.
* Root causes are those that can reasonably be identified. The investigation should be cost beneficial and root causes should be identified in a timely manner.
* Root causes are those that management has control over to remediate. Identifying “severe weather” as root cause for data center power failure is not appropriate since management has no influence on severe weather conditions.
* Root causes are those for which effective recommendations for preventing recurrence can be implemented. Recommendations should directly address the root causes identified.

There are four major steps in root cause analysis:

* Data collection
* Causal factor determination and charting
* Root cause identification
* Recommendations generation and implementation

The first step is to gather complete and meaningful data in order to understand the event. Documentation such as the <Security Incident Intake Form> and <Security Incident Response Tracking Form> along with evidence of the incident will help determine the nature and ultimately the cause of incident.

## Evidence Gathering and Handling

In some cases, evidence must be gathered for legal proceedings, and should therefore be documented and preserved according to all applicable laws and regulations. The Legal Department should be consulted with to determine procedures for gathering and handling evidence so that it is admissible in court.

Whenever evidence is handed off from one entity to another, chain of custody forms must be maintained to document the details of evidence transfer. The forms should contain the following information:

* Detailed identifying information about the piece of evidence (e.g., serial number, model number, IP address)
* Name, title, and contact information for each individual who handled the evidence
* Time and date of evidence handling
* Location of evidence at all times

For forensic investigations, it is best to acquire evidence as early as possible. System images and other forms of evidence are most valuable before any changes have been made for analysis or containment. Once an incident is detected and verified, the SIRT should coordinate with the Legal Department to ensure the proper handling of forensic evidence.

The <Chain of Custody Form or insert other form> should be used to record the initial receipt and any movement of evidence items. This form should be attached to each evidence item such as a laptop, a hard drive, or an evidence bag containing paper records.

Risk Assessments and related documentation demonstrating low probability of compromise to PHI will be kept on file for a minimum of six years.

## Lessons Learned

In order to learn from the incident and reduce the risk of similar incidents occurring in the future, it is important that the SIRT members maintain detailed and accurate records of all actions taken during the incident handling. Each SIRT member involved in the incident handling must record his or her own actions.

The SIRT should hold a “lessons learned” meeting within <10 business days or insert appropriate timeframe> with all involved parties after a major security incident, and periodically after minor incidents. A Lessons Learned Evaluation Form is included in Appendix B.

Results from lessons learned will be incorporated into future Plan revisions and staff trainings as appropriate to promote continuous improvement and preparation for future incidents.

# References

## Applicable regulations and standards:

* HIPAA §164.308(a)(6)(i): Security Incident Response
* HIPAA §164.308(a)(6)(ii): Response and Reporting
* HHS 405(d): Aligning Health Care Industry Security Approaches. <https://405d.hhs.gov/protect>
* NIST SP 800-66: Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)
* ISO/IEC 27002: 2005 Section 13 Information security incident management
* ISO/IEC 27001: 2005 Section A.13 Information security incident management

## Other Sources:

* “[Chapter 08 Incident Response Report Template](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response-Appendix-K-Incident-Report-Template?DLPage=4&DLEntries=10&DLSort=0&DLSortDir=ascending).” Centers for Medicare & Medicaid Services (CMS). Last updated July 19, 2021.
* “Healthcare System Cybersecurity, Readiness & Response Considerations.” Administration for Strategic Preparedness and Response (ASPR). Updated October 2022. <https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf>
* “[Incident Response Plan (IRP) Basics](https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf).” Cybersecurity & Infrastructure Security Agency (CISA).
* “National Cyber Incident Response Plan.” Department of Homeland Security. December 2016. <https://www.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf>
* “[NIST SP 800-86](https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response): Guide to Integrating Forensic Techniques into Incident Response.” National Institute of Standards and Technology. Last updated September 1, 2006.
* “[NIST SP 800-184](https://csrc.nist.gov/publications/detail/sp/800-184/final): Guide for Cybersecurity Event Recovery.”National Institute of Standards and Technology. Last updated December 2016.
* “[SHARING CYBER EVENT INFORMATION: OBSERVE, ACT, REPORT](https://www.cisa.gov/sites/default/files/publications/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf).” Cybersecurity & Infrastructure Security Agency (CISA).
* Coordinated Healthcare Incident Response Plan (CHIRP)” Healthcare & Public Health Sector Coordinating Councils. Last updated June, 2023, “<https://healthsectorcouncil.org/wp-content/uploads/2023/07/HIC-CHIRP-FINAL_1.pdf>

# Appendix A: *SAMPLE* Security Incident Response Checklist

The following is a sample checklist that can be used to guide general security incident handling. Specific information for each phase are located in the corresponding sections of this plan.

| **Step** | **Action** | **Owner** | **Status** | **Completed by** |
| --- | --- | --- | --- | --- |
| **Detection and Reporting** |
| ***Identification*** |
|  | Receive notice of security event.  | <Helpdesk> |  |  |
|  | Complete the [**Security Incident Intake Form**](#D1). |  |  |  |
|  | Determine validity of incident and type (e.g., denial of service, malware, inappropriate use). |  |  |  |
|  | Assign initial priority rating (e.g., Urgent, High, Medium, Low). |  |  |  |
| ***Triage*** |
|  | If the <CISO> is not yet aware of the incident, notify the <CISO> by sending an e-mail to <Email Address>  |  |  |  |
|  | Acknowledge the receipt of incident notification. |  |  |  |
|  | If the <CISO> does not acknowledge the incident within the appropriate time period, escalate the incident to the <CISO> via mobile phone and e-mail. |  |  |  |
|  | If the <CISO> does not acknowledge the incident within the appropriate time period, directly contact the SIRT via e-mail distribution list and contact numbers. |  |  |  |
|  | If suspected Breach, coordinate with Legal and Communications Manager> (Breach Response) |  |  |  |
|  | Notification of Insurance Policy if needed.  |  |  |  |
| ***Analysis*** |
|  | Complete the **Security Incident Tracking Form**. |  |  |  |
|  | Analyze the incident based on the type. |  |  |  |
|  | Adjust the priority rating if necessary and assign a severity rating. |  |  |  |
|  | If the incident is classified as **Severity 1 or Severity 2**, notify, and involve the SIRT via the e-mail distribution list and call. |  |  |  |
|  | Hold an incident response meeting with all appropriate SIRT members to discuss the issue and determine appropriate containment, eradication, and recovery actions. |  |  |  |
| **Containment, Eradication, and Recovery, and Recovery** |
|  | Determine containment, eradication and recovery strategy depending on the type of incident. |  |  |  |
|  | Schedule follow-up meetings based on the priority of the incident. |  |  |  |
| **Post-Incident Activities** |
|  | Gather evidence and track its location using the <Chain of Custody Form> in case a formal investigation is initiated. |  |  |  |
|  | Perform root cause analysis. |  |  |  |
|  | Hold a "lessons learned" meeting within <10 business days or insert alternative timeframe> of the incident closure.  |  |  |  |
|  | Revise Plan and other documentation to incorporate lessons learned. |  |  |  |
|  | Communicate updates to staff as appropriate.  |  |  |  |

# Appendix B: Communications

|  |
| --- |
| TEMPLATE INSTRUCTIONS AND NOTES (DELETE BEFORE PUBLISHING)* Each organization should have a tailored communication plan that includes pre-approved communication templates that can be easily leveraged to inform staff and stakeholders in the appropriate manner. This includes press responses and response to requests from media.
* Review your cyber-liability plan to ensure requirements for contacting and communicating with your cyber-liability provider are incorporated into your communications. Plans vary in requirements.
* Consider use of an independent mass notification system to ensure immediate communication with key stakeholders and staff immediately in the event of a cyber incident and during downtime.
* Identify an out-of-band communication mechanism that can be used securely in the event of internal communication compromise.
* Advise staff and leadership not to speculate as to the cause and effect of a cyber incident over email, which can be discoverable in subsequent civil actions, or to media outlets (or other public venues) where information can be exploited.
 |

## Communications Management

Upon confirmation of a security incident, the <CISO or insert role> will coordinate with the <Communications Manager or insert role> to review and execute the necessary internal and external communications to appropriately inform affected parties in a timely manner.

## Internal Incident Status Reporting

Periodically during the response of the SIRT to a security incident, the <CISO or insert role> shall inform the Executive Team of the status of the response to the Security Incident in as appropriate with the severity level that provide technical details, including:

* Current Risk
* Users Impacted (some, many, all?)
* Services Impacted (production, enterprise apps, other)
* Timeline of events
* Mitigation steps that have been taken
* Current status of the incident
* Next steps

## Communications Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Group or Stakeholder Name** | **Severity** | **When to Engage** | **Method of Engagement** | **Frequency of Communications** | **Tools and Templates** |
| Executive Leadership | **Sev 1** | Within 30 minutes | Phone Call  | Status every 30 minutes via email | * Status Meetings
 |
| **Sev 2** | Within 2 hours | Email and phone call | Status every 2 hours via email |  |
| **Sev 3** | Within 4 hours | Email | Status every 8 hours via email |  |
| <Role> | **Sev 1** |  |  |  |  |
| **Sev 2** |  |  |  |  |
| **Sev 3** |  |  |  |  |
| <Role> | **Sev 1** |  |  |  |  |
| **Sev 2** |  |  |  |  |
| **Sev 3** |  |  |  |  |
| <Role> | **Sev 1** |  |  |  |  |
| **Sev 2** |  |  |  |  |
| **Sev 3** |  |  |  |  |
| <Role> | **Sev 1** |  |  |  |  |
| **Sev 2** |  |  |  |  |
| **Sev 3** |  |  |  |  |

## Communication Templates and Approval Process

<Communication Templates> have been pre-approved for use in the event of a security incident. The <Communications Manager or insert role> will be primarily responsible for disseminating communications in coordination with the SIRT team as appropriate.

Templates are reviewed and revised to align with ongoing needs of the organization. Communication templates must be <insert review and approval process.>

Current templates can be found at: <insert location>

## Breach Notifications

### General Breach Notification

If after a risk assessment has been conducted, and it is determined that there has been a breach of unsecured PHI, <CISO or insert other role> will notify the appropriate individuals and agencies in accordance with the approved Communications Plan.

If the <Privacy Officer or insert other role> determines that the organization will need to provide notice to the patients, the <Privacy Officer or insert other role> will provide the notice as soon as can reasonably be accomplished and not more than 60 days from the date the breach was discovered or should have been discovered.

Breach notification will not occur until the documented investigation and the type of data breached is reviewed by legal counsel to determine if notification is required pursuant to existing contracts, applicable Business Associate Agreements, or federal or state law.

Notification may be delayed if law enforcement is notified and law enforcement requests and the Organization does not legally oppose such a request, to assist with the investigation process.

Notification will be made in accordance with applicable contract requirements (if applicable), Business Associate Agreements entered into with other entities (if applicable), and federal and state laws.

### Timing of Notification

The <Privacy Officer or insert other role> will consult with legal counsel after it appears that a breach of unsecured PHI has occurred, unless a law enforcement official determines that this consultation will impede a criminal investigation or cause damage to national security. The <Privacy Officer or insert other role> will initiate the Communications Plan based on the determined impact. The <Privacy Officer or insert other role> will make the notification required by the <Breach Notification Policy or insert other policy> to the patients affected without unreasonable delay and in no event later than sixty (60) calendar days after <CISO or other role> determines that a breach has occurred.  For purposes of this notification timeframe, a breach is deemed to have been discovered on the first day that such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a Workforce Member or agent of the organization.

### Method of Notification

<Privacy Officer or insert other role> will provide notice of a  breach to affected individuals in writing, by first class mail, sent to the last known address of the individual. If an individual has specified a preference for electronic mail notices, such notice shall be made via electronic mail.  If the <Privacy Officer or insert other role> knows the individual is deceased and has the address of the next of kin or personal representative of the individual, the <Privacy Officer or insert other role> will provide notification by first-class mail to either the next of kin or personal representative of the individual. The foregoing notifications may be provided in one or more mailings as information is available.  In cases deemed by the <CISO or insert other role> to require urgency because of the possible misuse of unsecured PHI, the Organization may provide information to individuals by telephone or other means, as appropriate, in addition to the written notice required under the <Breach Notification Policy or insert other policy>.

If <Organization> has insufficient or out-of-date contact information that precludes written notification to the individual in the manner described above, <Organization> will provide a substitute form of notice reasonably calculated to reach the individual.  Such substitute notice will not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of an individual known by <Organization> to be deceased.

In cases where there is insufficient or out-of-date contact information to provide written notice required under the <Breach Notification Policy or insert other policy> for fewer than ten (10) individuals, the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

In cases where there is insufficient or out-of-date contact information to provide written notice required under this Breach Notification Policy for ten (10) or more individuals, <Organization> will either; (1) make a conspicuous posting for a period of ninety (90) days on the home page of its website, or (2) make a conspicuous notice in a major print or broadcast media, including major media in the geographic area(s) where the individuals affected by the breach likely reside.  Such postings and notices will include a toll-free phone number where an individual can learn whether the individual’s unsecured PHI may be included in the breach.

If a breach of unsecured PHI by <Organization> involves more than 500 residents and <Organization> cannot demonstrate low probability that the PHI has been compromised based on a risk assessment using the four factors detailed in 45 C.F.R. 164.402(2), then in addition to the notice described above, <Organization> will provide a breach notice to prominent media outlets serving the geographic area(s) of the individuals affected by the breach.

If a breach of unsecured PHI involves 500 or more individuals and <Organization> cannot demonstrate low probability that the PHI has been compromised based on a risk assessment (same as above), then in addition to the notice described above, <Organization> will notify the Secretary of Health and Human Services (HHS) of the breach in the manner specified by the Secretary.

### Content of Notification

All breach notices made by <Organization> pursuant to the <Breach Notification Policy or insert other policy> will be written in plain language and will, to the extent possible, include the following information:

* A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
* A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, diagnosis, diagnosis code, or other types of information that were involved);
* The steps individuals should take to protect themselves from potential harm resulting from the breach;
* A brief description of what <Organization> is doing to investigate the breach, mitigate harm and losses, and protect against any further breaches; and
* Contact procedures for individuals to ask questions or learn additional information, including a toll-free telephone number and an email, website, or postal address.

### Log of Breach Events

<Privacy Officer or insert other role> will maintain a log of all events constituting a breach of unsecured PHI involving less than 500 individuals, and after consultation with legal counsel, will submit such a log to the Secretary on an annual basis of such breaches occurring during that year, not later than sixty (60) days after the end of that calendar year.

### Business Associate Notifications

Third party vendors that use and disclose PHI on behalf of <Organization> (Business Associates) are required to report any breach involving unsecured PHI to <Organization> within <three (3) business days of discovery of the breach or insert other timeline>.

Business Associates are required to include the following information in the report to <Organization>:

* Individual’s names or a unique identifier if that is all that is in the possession of the third-party entity and contact information for the individual, if available;
* Individual or individual’s next of kin’s (if the individual is deceased) contact information (if known);
* A description of the incident in general terms;
* The approximate date of the breach of security and the date that the third party vendor entity discovered the breach;
* The type of PHI breached;
* Brief description of what the third party vendor is doing to investigate the incident, mitigate damages and protect against like breaches in the future; and
* A description of the incident in general terms.

At <Organization> discretion, third-party vendors will be responsible for individual notification if the breach.

### Cyber-Liability Provider Notification Process

<If applicable, insert any specific notification procedures required by your cyber-liability plan and provider.>

### State Law Breach Notification Process

<If applicable, insert any specific notification procedures required by State law.>

## Voluntary Reporting to the Federal Government

Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, or any of the federal agencies listed in below. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders to respond to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation, in addition to voluntarily reporting the incident to an appropriate federal point of contact. Federal agencies also collaborate with state, local, territorial and tribal government organizations as appropriate given the nature of the cyber incident.

WHAT TYPES OF ACTIVITY SHOULD YOU SHARE:

Unauthorized access to your system

* Denial of Service (DOS) attacks that last more than 12 hours
* Malicious code on your systems, including variants if known
* Targeted and repeated scans against services on your systems
* Repeated attempts to gain unauthorized access to your system
* Email or mobile messages associated with phishing attempts or successes.
* Ransomware against Critical Infrastructure, include variant and ransom details if known

FEDERAL AVENUES FOR SHARING:

* **FBI Field Office Cyber Task Forces:** http://www.fbi.gov/contact- us/field
* **Internet Crime Complaint Center (IC3):** http://www.ic3.gov
* **Cybersecurity & Infrastructure Security Agency (CISA):** To report anomalous cyber activity and/or a cyber incident to CISA, email report@cisa.gov or call (888) 282-0870. You may also report ransomware incidents via the CISA Incident Reporting System and/or through the FBI Internet Crime Complaint Center (IC3).
	+ Note: \*\*CISA partners with the Anti-Phishing Working Group (APWG) to collect phishing email messages, mobile messages and website locations to help people avoid becoming victims of phishing scams. You can share phishing info with CISA by sending the phishing email to phishing-report@us-cert.gov.

# Appendix C: Security Incident Response: Lessons Learned Evaluation Form

The purpose of the Lessons Learned Evaluation form is to capture steps taken in response to a security incident and capture what was effective and not effective during the events of a security incident. Each form should be saved with its corresponding incident to be tracked and to also be used to prevent future occurrences of similar incidents.

|  |  |
| --- | --- |
| Incident ID or Ticket # |  |
| Event Description |  |
| Incident Closure Date |  |
| Lessons Learned Session Date |  |
| Participants |  |
| Summary of Resulting Actions |  |

| **Question** | **Notes and Considerations** |
| --- | --- |
| 1. Was the incident response appropriate? How could it be improved?
 |  |
| 1. Was every appropriate party informed in a timely manner?
 |  |
| 1. Were the incident response procedures detailed and did they cover the entire situation? How can they be improved?
 |  |
| 1. Have changes been made to prevent reoccurrences of this incident? (Systems patched, systems locked down, passwords changed, anti-virus updated, email policies updated, etc.)
 |  |
| 1. Could an additional policy have prevented this incident?
 |  |
| 1. Was a policy not followed which led to this incident? If so, what can be changed to ensure the appropriate policy is followed in the future?
 |  |
| 1. What other lessons have been learned from this experience?
 |  |
| 1. What does this incident tell us about the current threat landscape?
 |  |
| 1. Other Notes or Identified Next Steps
 |  |

# Appendix D: Security Incident Play Books

|  |
| --- |
| TEMPLATE INSTRUCTIONS AND NOTES (DELETE BEFORE PUBLISHING)* 405(d) offer some additional samples of Incident Response Plays for IR Playbooks which can be found at <https://405d.hhs.gov/Documents/tech-vol2-508.pdf>
 |

## Ransomware Playbook

Ransomware-specific response procedures can be found at: <insert link>

# Appendix E: Example Containment Strategy

**Example Containment Strategy (From HIC-CHIRP)**

<https://healthsectorcouncil.org/wp-content/uploads/2023/07/HIC-CHIRP-FINAL_1.pdf>

|  |  |
| --- | --- |
| **Containment Strategy** | **Containment Rationale** |
| Disconnect the organization from the public internet | • Widespread malware infection utilizing Command and Control infrastructure or with the potential to leak data • Potential active threat actor in the environment with unknown point of access |
| Disconnect the organization from vendor / partner / affiliate / clinic WAN / VPN connections | • Possibly wormable malware infection with potential to spread to third parties • Potential third-party source of threat actor access |
| Disconnect internal network at major segmentation points • Medical Device Network • Patient Monitoring Network • Lab Device Network • Facilities Network | • Possibly wormable malware infection with potential to spread to sensitive systems |
| Mass quarantine of infected endpoints through EDR platform | • Possibly wormable malware infection with potential to spread to additional endpoints |
| Disconnect backup systems from the network | • Unchecked data encryption/destruction occurring • Potential active threat actor in the environment with the capability to pivot to attack backup systems |

Organizations should add, remove, or update the table based on internal capabilities and organizational structure. Developing playbooks separate from this plan to execute each strategy is strongly encouraged.

Organizations should refine or expand containment strategies once impact assessments have been conducted.