Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Respond & Recover

Health Industry Cybersecurity -

Coordinated Healthcare Incident Response Plan (CHIRP)

JUNE 2023

Table of Contents

Introduction

Various groups have published material for the technical response process to a cybersecurity incident. These plans and templates provide universal guidance that can be used across industries to inform how to detect, contain, respond, and recover from a cybersecurity incident. This template does not seek to replicate or replace those existing resources. Unaddressed by the available guidance is the rippling operational impact on patient care unique to a healthcare cybersecurity incident that expands the potential impact from not only loss of data or revenue but loss of patient safety. A focus on patient safety and preparations to handle operational disruptions are not foreign concepts to healthcare delivery organizations.

Emergency Management planning prepares an organization to handle an array of hazards that could negatively impact patient care, but these plans are generally focused on kinetic rather than digital threats. Business continuity planning and downtime procedures address continuity of care in the absence of critical technology, but these plans tend to be built around general IT outages and cannot fully address the nuanced challenges of a cybersecurity incident outage. Healthcare Delivery Organizations have many of the parts and pieces needed to respond to a cybersecurity incident but guidance is missing on how to tie all of these separate components together. This template seeks to serve as the cog that can be installed in the machine to allow all of the components to run together as a Coordinated Healthcare Incident Response Plan.

This document is a template. It is not intended to be directly usable to manage a response as-is. Sample content is provided throughout the template as a starting point, but it is expected that managers of this tool will use it as a guiding document to develop a plan tailored to their own organization. Plan guidance is included to help managers of the tool understand the purpose of each section while conducting this planning work. Plan guidance sections are formatted differently from template material for clarity and to allow enterprises to easily remove these sections in their final plan.

This document is also a ***planning companion to the operational and response guidance*** of the Health Industry Cybersecurity Operational Continuity - Cyber Incident (HIC-OCCI), also published by the Health Sector Coordinating Council.

All incident response plans should be developed with appropriate consultation with all essential stakeholders both within and outside of the organization, consistent with enterprise policies and legal and compliance requirements.

About the Health Sector Coordinating Council Cybersecurity Working Group

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Cybersecurity Working Group (CWG) is a standing working group of the HSCC, composed of more than 400 industry and government organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

Acknowledgments

The Health Sector Coordinating Council expresses its gratitude to the many member representatives who worked on the Incident Response Business Continuity Task Group and contributed significant hours and thought leadership to the development of this resource.

In particular, we wish to thank the following individuals who volunteered as a "Strike Force" to draft the content in this document. This group met weekly over the course of a year to develop, review, solicit and adjudicate feedback and format for ease of use. The HSCC is indebted to their thought leadership, energy and commitment to the operational health of the sector.

Mike Caudill (co-lead)
Duke Health

Nathan Couture (co-lead)
The University of Vermont Health Network

Garrett Hagood (co-lead)
Coastal Bend Regional Advisory Council (CBRAC)

Darrell Hall (co-lead)
U.S. Department of Health and Human Services, Health Sector Cybersecurity Coordination Center (HHS HC3)

Lisa Bisterfeldt
St. Luke's Health System

Hazel Chappell
ishca health

Brindusa Curcaneanu
Nevro

Philip Curran
Cooper University Healthcare

Chris Graham
Presbyterian Healthcare Services

Andrea Greene-Horace
U.S. Department of Health and Human Services, Centers for Medicare & Medicaid Services (HHS CMS)

Karen Habercoss
The University of Chicago Medicine and Biological Sciences

Mark Jarrett
Northwell Health

Scott Lagger
Edward-Elmhurst Health

Steve Landes
Abbott

Mary Massey
California Hospital Association

Brady Miller
Methodist Le Bonheur Healthcare

Kirsten Nunez
Intermountain Health

Brian O'Neill
Northwell Health

Mitch Parker
Indiana University Health

Skip Skivington
Kaiser Permanente

Nastassia Tamari
Becton, Dickinson, and Company

Kristy Westphal
HealthEquity

Plan Governance

Plan Guidance

The coordinated response plan should be governed in accordance with organizational document management procedures to ensure it remains accurately aligned to other plans, procedures, and organizational structures. Suggested content areas for plan governance exist within the template, but organizations should tailor as appropriate to align with their organizational document management templates.

Scope

This plan is applicable to the entirety of [Organization Name], including affiliates, associates, and otherwise Registered Holdings. The purpose of this document is to promote a consistent coordinated response to disruptive cyberattacks affecting interconnected systems and networks. The plan outlines the coordinated process to respond to a cybersecurity incident that could impact patients, staff, visitors, or others with the potential to cause significant disruption or impair the ability to deliver patient care.

This plan is designed to interact with and coordinate activities from various other organizational plans including Cybersecurity Incident Response Plans, Cybersecurity Playbooks, Disaster Recovery Plans, Hospital Incident Command Procedures, Business Continuity Plans, Emergency Management Plans, and Downtime Procedures. This plan is not intended to replace or circumvent any other detailed plans. More detailed subject area plans should be deferred to when appropriate.

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 Cybersecurity Incident Response Plan and/or Playbooks.

Authority

Included within this plan are predefined actions associated with authorizing groups or individuals. Where defined, these authorities are made explicit through the regular review and approval of this plan. Where decision authority is not explicitly defined or not well understood, decision authority for response actions will default to the Cybersecurity Response Governance Team as defined within this plan.

Exercise and Evaluation

To ensure the accuracy and operationality of this plan, it should be exercised, and evaluated on a regular basis. Exercises should be driven by measurable objectives and can be completed at the team, department, or facility level. Examples of exercises could include workshops, tabletop exercises, simulation drills, or functional / full scale exercises. A debrief or after-action review should be completed post-exercise in which opportunities and action items are identified to ensure ongoing maturity and continuous improvement of response processes and this plan for business sustainability.

Review and Approval

This plan should be reviewed on an annual basis or after a response to any cybersecurity incidents or material changes to organizational structures or associated detailed plans. The plan is approved by [Approving Authority] and thus confers the authorities within.

Coordinated Response Plan

Plan Guidance

For broadest applicability, the below plan is organized by subject area rather than organizational department. Based on the size and structure of an organization, multiple subject area responsibilities may be shared by a single group or individual or an individual subject area may spread across multiple groups. An organization may choose to condense or expand this plan to match its organizational structure if a more direct responsibility mapping is desired. The high-level milestone activities are recorded here for each subject area with the expectation that detailed activities are recorded in respective plans (i.e., Cybersecurity Incident Response Plan and playbooks, Breach Response Plan, Downtime Procedures, Organizational Policies, Standard Procedures, and Hospital Incident Command plans). Activities within a row are considered appropriate to occur in parallel. Subject areas should not advance to milestone activities in further rows until the milestones from other subject areas are also completed and the areas have synchronized. This approach prevents unnecessary linear blocking of timely activities while also reducing risk of adverse effects from taking some actions too soon. An organization should review the milestones below and carry out a comparative analysis of internal individual detailed plans and tailor the Coordinated Response Plan as appropriate for their own organization.

Cybersecurity Response	Information Technology Recovery	Operations and Emergency Management	Communications	Privacy, Legal, and Risk Management
Catastrophic Cybersecurity Incident Identification				
• Activate Cybersecurity Incident Response Team and Governance Team • Conduct initial cyber assessment • Execute initial containment strategies	• Activate IT Incident Command Center • Conduct initial technical assessment	• Activate Hospital Incident Command • Initiate Downtime Procedures • Establish initial incident objectives (mandatory	• Send initial internal General IT Outage communication • Activate Out of Band Internal Command Communications • Activate situational reporting system(s) to facilitate internal	• Begin tracking for potential privacy, regulatory, legal, or other risk impact

		communication objective)	incident information sharing and summary reporting	
Command Center Synchronization – Assessment and Response				
• Conduct full cyber impact assessment • Refine or expand containment strategies	• Activate pre-identified critical standalone interim systems • Conduct full technical impact assessment	• Activate extended downtime procedures and Business Continuity Plans • Reallocate resources from paused operations to support downtime procedures	• Update internal communications with known scope of impact • Issue initial external communications to patients and partners • Activate Call Center procedures and scripts • Initiate internal and external inquiry triage process	• Begin Law Enforcement, Government, and Regulatory notifications • Notify Cyber Insurance
Command Center Synchronization – Eradication and Continuity				
• Establish and execute eradication plan • Validate eradication	• Execute rebuild and recovery activities • Validate technical recovery	• Activate interim solution request process	• Begin full media relations activities	• Consult and guide extortion decisions
Command Center Synchronization – Restoration and Recovery				
• Lift containment strategies • Begin full forensic analysis	• Activate integrations • Deactivate interim systems	• Return to standard operations • Begin data backload from downtime procedures downtime procedures	• Update internal and external communications with return to standard operations procedures and scripts • Initiate internal and external inquiry triage process	
Command Center Synchronization Closeout				

• Establish risk mitigation plans • Complete cyber response review • Update cyber response plans & disseminate for approval	• Complete technical recovery review • Update technical recovery plans	• Complete Emergency Management and Downtime Procedures review (Hotwash?) • Conduct After Action Review (AAR) • Update Emergency Management plans and Downtime Procedures	• Complete crisis communications review • Update crisis communication plans	• Conduct Breach Analysis • Complete legal and regulatory notification • Determine and execute handling of follow up privacy and legal inquiries

Disruptive Cybersecurity Incident Identification

Plan Guidance

A large-scale coordinated response is not appropriate for all cybersecurity events and incidents. Isolated cybersecurity events are best handled by detailed Cybersecurity Playbooks. Even moderate cybersecurity incidents impacting only a small number of devices with limited operational impact can be handled by the standalone Cybersecurity Incident Response Plan. Likewise, privacy and other regulatory incidents and potential breaches without an operational impact are best handled by a distinctly separate dedicated Incident and Breach Response Plan (with the exception of breach incidents that require mitigation or containment activities that result in broad operational impact).

This section sets forth the process and criteria for identifying a cybersecurity incident as appropriate for the activation of the coordinated response plan. The following template provides example roles, responsibilities, and decision authority as well as criteria to support the decision. These roles and associated criteria should be tailored based on organizational structure and risk tolerances to business disruption.

Secondary contact information not reliant on any internal systems should be identified for each role in the event that communication systems are impacted.

Incident Identification: Roles and Responsibilities

Plan Guidance

Modify the table below to align with titles, roles, and responsibilities of your organization.

Name	Responsibility/Authority	Contact
Entire Workforce	Report any suspicious activity to the Cybersecurity Team	N/A
Cyber Security Team	Review cybersecurity activity reports and event alerts to identify potential incidents. Raise incidents to CISO or delegate.	Phone: Email: Portal URL:
Primary: **Firstname Lastname** **Delegate:** **Firstname Lastname**	Review details of the cybersecurity incident against decision criteria and recommend coordinated response activation	Phone: Email: Secondary Contact:
Primary: **Firstname Lastname** **Delegate:** **Firstname Lastname**	Authorize the activation of the coordinated response plan and notify Hospital Incident Command	Phone: Email: Secondary Contact:

Disruptive Incident Criteria

Cybersecurity incidents can vary in size and scope. This plan is intended to be implemented following a disruptive cybersecurity event that results in a business interruption or disturbance in which downtime or continuity plans are implemented. The following criteria shall be considered when evaluating a cybersecurity incident for coordinated response plan activation:

- A disruptive cybersecurity attack where business-critical information systems are unavailable
- A disruptive cybersecurity attack where a significant portion of endpoints (desktops/laptops/mobile devices) are unavailable
- A disruptive cybersecurity attack on non-business-critical systems with significant potential to spread to business-critical information systems
- A substantiated immediate threat of disruptive cybersecurity attack with significant potential to impact business-critical information systems or a large portion of endpoints
- A data theft cybersecurity attack that warrants disruptive responsive actions to contain and/or mitigate the attack that will impact business-critical information systems or a large portion of endpoints

Cybersecurity Response Governance Team

Plan Guidance

Wherever possible, it is recommended to define targeted decision authority in advance within elements of both the coordinated response plan and specific area response plans, but there may be unpredicted decisions required during a response due the number of variables involved in a cybersecurity incident. Predefining a Cybersecurity Response Governance Team ensures a consistent resource to arbitrate matters and render efficient decisions with adequate authority to decide on behalf of the organization. The roster for the Cybersecurity Response Governance Team should be established in advance 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.

Some suggested role recommendations are made in the table below, but responsibilities and authorities vary significantly between organizations and the table should be tailored based on specific organizational structure and roles.

Incident Governance Team

Name	Responsibility/Authority	Contact
Firstname Lastname Title:	Cybersecurity risk implications	Phone: Email: Secondary Contact:
Firstname Lastname Title:	Technology recovery and resiliency implications	Phone: Email: Secondary Contact:
Firstname Lastname Title:	Legal risk implications	Phone: Email: Secondary Contact:
Firstname Lastname Title:	Human resources / staffing implications	Phone: Email: Secondary Contact:
Firstname Lastname Title:	Patient / Customer risk implications	Phone: Email: Secondary Contact:

Firstname Lastname Title:	Privacy, compliance, and regulatory impact implications	Phone: Email: Secondary Contact:
Firstname Lastname Title:	Clinical operations implications	Phone: Email: Secondary Contact:
Firstname Lastname Title:	Business operations implications	Phone: Email: Secondary Contact:
Firstname Lastname Title:	Financial implications	Phone: Email: Secondary Contact:
Firstname Lastname Title:	Supply Chain implications	Phone: Email: Secondary Contact:
Firstname Lastname Title:	Public Relations, Communications	Phone: Email: Secondary Contact:
Firstname Lastname Title:	Emergency Management / Operational Resiliency	Phone: Email: Secondary Contact:
Firstname Lastname Title:	Physical Security implications	Phone: Email: Secondary Contact:

Quorum and Voting

For the purposes of making decisions and authorizing cybersecurity response activities, a quorum of the Cybersecurity Response Governance Team shall be considered [#] of [#] members present (physically or virtually) with approval voting based upon [plurality/majority/unanimity].

Command Center Synchronization

Plan Guidance

Operating in phases, allowing parallel work to occur for timeliness while also ensuring certain activities are serialized to avoid increased risks, is a key concept behind the coordinated response plan. Before moving from one phase to the next, it is important to synchronize across the subject areas to ensure all phase activities are complete and transfer necessary knowledge to enable activities in the next phase. Synchronization within phases is also beneficial to reduce uncoordinated information gathering and speed identification and resolution of roadblocks to recovery. The most effective way to facilitate the synchronization across subject matter areas is through the use of a command center structure. An organization may already have a command structure and cadence defined in Emergency Management or Hospital Incident Command plans which could be referenced here, but organizations should validate those plans appropriately provide coverage for the subject domains involved in a cyber event. For a smaller organization, a single command center might be appropriate to cover all subject areas. In a larger organization, dedicated command centers allow for more focused sessions with less risk of distractions. The example command center cadence provided here is for the latter, but a smaller organization might use this example as a guide for the single command center's agenda. Identifying meeting times and locations (which may be physical or virtual) in advance allows for Command Centers to immediately form without requiring new coordination during the event.

Cadence Slot	Command Center	Inputs	Outputs	Daily Meeting Schedule	Location
1	Cyber Incident Command	Results of cyber assessments and current threat activity	Remediation requirements and guidance on cyber risk status for recovery activities	6:00am 12:00pm 6:00pm	
2	IT Incident Command	Remediation requirements, cyber risk status, recovery activity status	Guidance for IT recovery and remediation teams on next activities. Technical service availability status for Hospital Incident Command.	6:30am 12:30pm 6:30pm	

3	Hospital Incident Command	Technical service status, clinical and business issues requiring interim solutions	Establishment and tracking of incident objectives based on inputs. Maintenance of situation summary. Incident Action Plan (IAP) documentation. Coordination of incident response and recovery. Prioritized interim solution requests for risk assessment, communications guidance, guidance for clinical and business units for triage and downtime procedures	7:00am 1:00pm 7:00pm	
4	Clinical and Business Unit Commands	Technical service status, triage guidance, downtime procedure updates, unit schedules and challenges	Triage and scheduling decisions, updated unit procedures and guidance	7:30am 1:30pm 7:30pm	

Communication Strategy

Plan Guidance

Communications are essential to keeping various teams aware and updated of incident actions. A collaborative and multi-disciplinary communication strategy should be developed prior to an incident. The communication strategy should include when specific notifications should occur and the responsible parties for providing that communication.

The following table provides a starting point for recommended external contacts during a disruptive cybersecurity incident. Key information beyond the contact information itself includes the expectations around timelines for notification and the expectations of what the organization may receive in support through the contact. Pre-

identifying a responsible party for each contact avoids omitting a contact or duplicating efforts. An organization should review the table for relevancy, remove or add external entities as appropriate, and update contact and responsible party information. A primary and secondary responsible party being named is recommended. The roles found here are suggested recommendations and should be updated according to organizational structure and responsibilities.

Key External Contacts

Entity	Contact Method	Timeline	Response Expectations	Responsible Party
IR Partner	[Entity Specific]	Contact immediately upon disruptive cybersecurity incident identification.	Expect support in managing responsive containment, investigation, and eradication activities.	Primary: Name: Firstname Lastname Role: CISO Secondary: Name: Firstname Lastname Role: CIO
FBI	[Entity's local FBI Field Office http://www.fbi.gov/contact-us/field]	Contact following initial cyber assessment.	The FBI's primary duty is the potential criminal investigation but may also provide beneficial information to support the investigation and containment activities including Indicators of Compromise and Threat Actor behavior patterns.	Primary: Name: Firstname Lastname Role: General Counsel Secondary: Name: Firstname Lastname Role: Associate General Counsel
CISA	https://www.cisa.gov/report OR report@cisa.gov	Contact following full cyber assessment.	CISA analyzes input from incident reports to create anonymized alerts for industry. Report will be most valuable following collection of pertinent information to the attack.	Primary: Name: Firstname Lastname Role: CISO Secondary: Name: Firstname Lastname Role: CIO
Cyber Insurance	[Entity Specific]	[Timeline variable based on entity coverage and agreements]	[Expectations variable based on entity coverage and agreements]	Primary: Name: Firstname Lastname Role: Director of Risk Management Secondary: Name: Firstname Lastname Role: Associate General Counsel

State AG Office/State Police/Other State Agencies	[Variable by State]	[Variable by State]	[Variable by State]	Primary: Name: Firstname Lastname Role: General Counsel Secondary: Name: Firstname Lastname Role: Associate General Counsel
HHS Office for Civil Rights	Breach Report Portal: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true	Without unreasonable delay, but no later than sixty (60) days from the discovery of a protected health information (PHI) breach	HHS OCR does not provide any response support.	Primary: Name: Firstname Lastname Role: Chief Privacy Officer, General Counsel, or Designated Outside Counsel
External Vendors/ Third Parties	[Entity Specific]	Contact after initial cybersecurity assessment is complete and the vendor impact is known.	[Expectations variable based on specific vendor and service provided]	[Entity Specific]

Containment Strategy

Plan Guidance

Targeted containment strategies (i.e., disconnecting an infected host from the network or disabling a compromised account) should be included in detailed cybersecurity response plans and playbooks, but during a disruptive cybersecurity incident more holistic broad scale containment strategies may be required. If such major containment strategies are not already recorded in a detailed plan, consider recording here. The following table recommends potential strategies, the rationale to activate, and the authorizing party to activate. Organizations should review the table and add, remove, or update based on internal capabilities and organizational structure. Developing playbooks separate from this plan to execute each strategy is strongly encouraged.

Containment Strategy	Containment Rationale	Authorizing Party
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	Primary: Name: Role: Secondary: Name: Role:
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	Primary: Name: Role: Secondary: Name: Role:
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	Primary: Name: Role: Secondary: Name: Role:
Mass quarantine of infected endpoints through EDR platform	• Possibly wormable malware infection with potential to spread to additional endpoints	Primary: Name: Role: Secondary: Name: Role:
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	Primary: Name: Role: Secondary: Name: Role:

Interim Solution Request Process

Plan Guidance

In the event of an extended IT systems outage, it may become necessary to implement interim technical solutions to facilitate critical organizational capabilities prior to full system restoration. Consider critical patient care services (certain forms of care simply cannot be safely delivered without supporting technical systems). Ideally, alternative systems are pre planned into downtime procedures, but in a complex healthcare delivery environment, it is likely that new interim solution needs will be identified during the incident. The decision to implement an interim solution must be carefully balanced against diverting resources to work on interim solutions which would be unfocused on eradication or recovery efforts. Depending on the proposed interim solution and current state of the technical environment, the interim solution may present unacceptable additional clinical or technical risk(s). The below table represents a proposed flow of considerations and authorizing roles to move an interim solution proposal forward. Organizations should update as appropriate to match organizational priorities and structure.

Step	Description	Authorizing Function
1	The interim solution proposal is reviewed at the local clinical level for appropriateness of clinical use and patient safety considerations. Only proposals that represent significant improvement in patient care without introduction of undue patient safety risk are moved forward for further consideration.	Clinical Chair or Delegate
2	The interim solution proposal is reviewed at the broad clinical governance level to ensure the patient care value of implementing warrants the diversion of resources from full recovery efforts. If multiple interim solution proposals exist, they are stack ranked by clinical value to enable the next steps to occur in priority order.	Hospital Incident Command
3	The interim solution proposal is reviewed for potential cyber risk with consideration of the nature of the proposal and the current state of containment and eradication activities. The cyber risk to both the interim solution from the overall environment and the risk to the environment from the interim solution are both considered. Regardless of patient care value, an interim solution with unacceptable cyber risk will not move forward.	CISO or delegate
4	The interim solution is resourced with the appropriate technical staff and implemented. If the solution cannot be implemented due to a technical limitation, this is communicated back to Hospital Incident Command for clinical coordination of the impact.	IS/IT Section Chief

Extortion Strategy

In the event of an extortion-based attack, it may be necessary to make timely and difficult decisions. Conversations at the executive leadership level should be conducted before an event to discuss and define an extortion strategy. During an incident, the following items should be considered in acting on the extortion philosophy.

- Level of confidence in encryption keys
- Status of usable back ups
- The scope / impact of the cybersecurity attack
- Level of downtime maturity and downtime processes for hospital / health system
- Anticipated recovery timeline