Operational Continuity-Cyber Incident (OCCI) Checklist

November 7th, 2024

Health & Public Health Sector Coordinating Council

PUBLIC PRIVATE PARTNERSHIP

Table of Contents

Executive Summary

Call to Action - Cybersecurity is Everyone's Responsibility

Cybersecurity must be an integrated as an essential part of patient care to adequately maintain patient safety and protect the sector's information and data. The Healthcare and Public Health (HPH) sector will always be a target of cyber criminals. Therefore, it is crucial that organizations leverage cybersecurity best practices not just as preventative tools, but also as tools to improve our ability to respond.

Cybersecurity is everyone's responsibility. It is the responsibility of every healthcare and public health organization, and each member of the workforce to ensure **cyber safety is patient safety**.

Impact of Cybersecurity Incidents

The impact of a cyber incident can have direct patient impact and have financial, regulatory, and cause reputation damage to an organization Patient data can also be impacted when attackers sell patient data on the black market. "Over 56 percent of healthcare respondents said that their organization had experienced at least one data breach in the past. Over a quarter of respondents from the healthcare sector reported experiencing a data breach within the last 12 months alone."[5] An independent study showed that healthcare cyber incidents greatly disrupt care in the form of "delays in procedures and tests that have resulted in poor outcomes, longer length of stay, increase in patients transferred or diverted to other facilities, increase in complications from medical procedures and an increase in mortality rate", with ransomware being the most likely to cause harm.[6]

While HPH sector organizations have made great cybersecurity gains in the past few years, cybersecurity criminals still have the upper hand, forcing our organizations to continue to heavily focus on defense. "When examining all cyber incidents with relevant data in 2022, on average, 96 days passed between the time a breach occurred to the time it was discovered. This represents a decrease of nearly 27% from 2021, when the average time to discovery was 132 days." While an improvement, this data demonstrates that bad actors still have months with patient's protected health information (PHI) and, therefore, months to potentially wreak havoc on our critical infrastructure networks.[3] This further highlights the need for organizations to be prepared to act and respond immediately once the threat is identified.

Cyber incidents have become more advanced and sophisticated. Cyber incidents have led to massive network or data breaches that can impact your organization for days or even months.

One report states over 40 percent of surveyed healthcare organizations have not yet implemented an Incident Response Plan (IRP) to account for the constant threats of phishing, ransomware, and cybersecurity vulnerabilities that plague the industry.[7] These statistics speak loudly enough. Failure to plan and act is simply not an option with the complexity and intensity of cybersecurity threats to the sector.

5 https://email.protenus.com/hubfs/Breach_Barometer/2023/BreachBarometer_Privacy_2023_Protenus.pdf
6 https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf
7 https://healthitsecurity.com/news/42-of-healthcare-organizations-do-not-have-incident-response-plans

Importance Of Cyber Preparedness for Cyber Resiliency

Effective security practices and controls, such as robust perimeter security, email security and access controls, play a crucial role in preventing, detecting, and responding to threats. To assist the HPH sector in identification and implementation of high impact cybersecurity practices, in January 2024, HHS through extensive collaboration with private and public sector partners, published a set of voluntary healthcare specific Cybersecurity Performance Goals (HPH CPGs). These HPH CPGs are a voluntary subset of cybersecurity practices that healthcare organizations should prioritize to strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety. They were built off the chassis of CISA's CPGs and informed by common industry cybersecurity frameworks, guidelines, best practices, and strategies (e.g., Healthcare Industry Cybersecurity Practices, National Institute of Standards and Technology (NIST) Cybersecurity Framework, HealthCare and Public Health Sector Cybersecurity Framework Implementation Guide, and the National Cybersecurity Strategy). The HPH CPGs directly address common attack vectors against U.S. domestic hospitals as identified in the 2023 Hospital Cyber Resiliency Landscape Analysis. Both the essential and enhanced HPH CPGs emphasize the importance of incident planning and preparedness activities, to include encouraging organizations to consistently maintain, drill, and update cybersecurity incident response plans for relevant threat scenarios.

Importance of Incident Planning and Response

In emergency departments across the nation, thousands of staff members stand at the ready to respond to any situation that comes through the door. The same philosophy needs to be applied to cybersecurity.

Organizations need to be prepared for any cyber event and stand ready to respond. When patient safety is on the line every second matters.

A Business Continuity Plan (BCP) is the documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption. An Incident Response Plan (IRP), on the other hand, is specifically focused on how an organization will respond to and manage specific incidents, often related to information security or cyber incidents. It provides a detailed framework for identifying, containing, mitigating, and recovering from security incidents like data breaches, malware attacks, or network intrusions.

Incident response planning is the foundation to minimize the duration and damage of security incidents. It is the strategy in place for an organization to identify stakeholders, improve recovery time, ensure continuity of care, reduce negative publicity, and increase patient confidence in the healthcare system.

Proper incident response planning is an essential element in the moments of an actual cyber incident. An IRP identifies the procedures that should be put in place at the first sign of a cybersecurity incident. While having an IRP may not prevent business disruption and technical downtimes, an IRP can shorten or lessen the impacts, which could include financial losses and degraded patient safety. Damage to the network could become overwhelming and result in attackers shutting down your network. Network shutdown will result in financial loss and can negatively impact patient care and safety.

How The OCCI Checklist Was Developed

Due to the prevalence and increase of cyber incidents, the Health Sector Coordinating Council (HSCC) Cyber Working Group (CWG) established an Incident Response/Business Continuity (IRBC) Task Group in 2022, that called for heightened awareness and immediate preparations against potential disruptions to healthcare delivery. The taskforce created the initial checklist with an accelerated development cycle. This was intended to anticipate the potential for an extended outage in the event of direct cyber incidents or collateral fallout and message this information to stakeholders as quickly as possible. The OCCI Checklist was released on April 29, 2022, by the HSCC as a resource developed by industry, for industry.

Acknowledging the importance of this resource, the IRBC Task Group made a request to the 405(d) Task Group to consider incorporating the OCCI Checklist under the 405(d) Program and re-releasing it as a joint product between HHS and HSCC. In early 2023, the 405(d) Task Group established a sub working group to review and update the OCCI Checklist. This iteration of the OCCI Checklist ran through the 405(d) review and clearance process, which included various review periods conducted by both industry and government stakeholders. This re-released joint public-private resource is the result of a true collaborative effort and represents the best collective thinking of public-private HPH cybersecurity and emergency management professionals.

About the OCCI Checklist

The Operational Continuity-Cyber Incident (OCCI) checklist serves as an action plan designed to potentially assist operational staff and executive management in effectively responding to and recovering from an extended enterprise outage caused by a severe cyber incident. **This checklist, an integral component of your broader Incident Response Plan (IRP), is specifically tailored to address the critical first 12 hours following a cyber event.** Its recommended operational procedures and tasks can be adjusted or refined to align with an organization's size, available resources, complexity, and capabilities. While it is recognized that Emergency Managers and individuals trained in the Hospital Incident Command System (HICS) are the primary audience - it is important to emphasize that this document serves as an inclusive resource. It offers small healthcare organizations, regardless of their familiarity with these terms and procedures, a valuable starting point and guidance to enhance their preparedness efforts.

How Can This Checklist Help Me?

The effects of a cyber event, such as a cybersecurity disruption in an information system or technology resource that may have an impact on organizational operations (including mission, capabilities, or reputation), can be overwhelming and leave many unknowns. The complexity of the HPH sector also adds additional considerations into any planning or response efforts. The intent of this OCCI Checklist is to provide organizations of all sizes with key **actionable and vetted steps that can be put into place at the first sign of a cybersecurity incident**. Whether you are a small organization or a larger integrated organization, the OCCI Checklist is organized from a role-based perspective. Each role aligns to tasks which an assigned staff member would be responsible for implementing in real time, within an HPH setting. In smaller health organizations, these critical roles may often be assigned as secondary functions, and the OCCI checklist is strategically designed to offer them comprehensive guidance on high-level responsibilities and actionable steps, should they find themselves assuming these roles during a cyber incident. This means that even

organizations with limited resources or personnel can effectively leverage the checklist to enhance their cybersecurity preparedness and response capabilities, fostering a proactive approach to mitigating cyber threats in the healthcare sector.

The checklist provides a flexible template for operational staff and executive management to respond to and recover from an extended enterprise outage due to a serious cyber incident. Its suggested operational structures and tasks can be modified or refined according to an organization's size, resources, complexity, and capabilities.

Having an IRP in place helps all critical stakeholders understand the lifecycle of a cyber incident and have rehearsed it at all levels of the business. This greatly prepares an organization to mitigate the damage of an incident.

How to Use This Checklist

The purpose of this document is to serve as a resource guide and support to Incident Command Activation and response actions in case of a Cybersecurity Incident resulting in an extended downtime event. Incident Command Activation, IRP for a cyber incident, refers to the process of formally initiating and organizing the response efforts when a cybersecurity incident occurs. **This document is meant to recommend or inform action from the Command team for the first twelve hours of the cyber incident.** The document was developed in alignment with the Hospital / Healthcare Incident Command System (HICS)[8] and includes recommended actions for the following Incident Command positions: Incident Commander, Medical Technical Specialist, Public Information Officer, Liaison, Safety Officer, Operations Section Chief, Planning Section Chief, Finance Section Chief, Logistics Section Chief, Information Technologies (IT) / Information Systems (IS) Section Chief, .

An organization should:

1. Review the checklist and begin to identify who in their organization should perform these roles.
2. The checklist should be distributed and reviewed to help make all participants are aware of their responsibilities. The urgency of each task should be communicated, as the checklist is more impactful if all participants are engaged and responsive.
3. When possible, identify a primary and secondary for each role.
4. Display the checklist in a pertinent location that is easily accessible and include it in an onboarding package to be distributed to new staff joining the HPH organization.
5. Review and update the checklist at least annually or after any cyber incident to revise or update the process.

To assist with the accuracy and operationality of this resource, 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 facilitate ongoing maturity and improvement of response processes and this plan.

8 https://files.asprtracie.hhs.gov/documents/epimn-module-2-understanding-hospital-ics.pdf ; https://aspr.hhs.gov/HealthCareReadiness/guidance/MSCC/Pages/Appendix-B-Incident-Command-System-for-Public-Health-and-Medical-Professionals.aspx

Operational Continuity-Cyber Incident (OCCI) Checklist Introduction

Developed for small organizations and larger integrated organizations, the OCCI Checklist is organized from a role-based perspective. Each role aligns to tasks which an assigned staff member would be responsible for implementing in real time, within an HPH setting. This checklist is intended to provide a flexible template for operational staff and executive management. It should be used to respond to (and recover from) an extended enterprise outage due to a serious cyber incident. Suggested operational structures and tasks can be modified or refined according to an organization's size, resources, complexity, and capabilities.

This checklist outlines recommended initial (first 12 hours) actions and considerations during a large scale cybersecurity incident impacting operations and patient care.

Command positions should be activated as they are needed. If a Command position is not activated, actions fall to the Incident Commander and can be delegated as appropriate. Position activation may depend on staff availability or the size and scope of the cyber incident.

Based on an assessment by Chief Information Officer, Chief Information Security Officer, and/or senior leadership, incident command may be activated.

The following pages will include Incident Command positions and their respective responsibilities:

- Incident Commander
- Medical Technical Specialist
- Public Information Officer
- Liaison
- Safety Officer
- Operations Section Chief
- Planning Section Chief
- Finance Section Chief
- Logistics Section Chief
- Information Technologies (IT) / Information Systems (IS) Section Chief

Incident Commander

Role: Provides overall strategic direction on all site-specific response actions and activities.

- ❑ **Formal declaration of a cyber incident**
  - Define size and scale of command activation
  - Define type of command (in person, virtual, single, multiple)
  - Define communication modalities based on cyber incident
- ❑ **Identify cyber incident scope and obtain situational awareness**
  - Identify Scope – One site/multiple sites/isolated outage/full network outage
  - Assume it is a malicious cybersecurity incident until proven otherwise
  - Situational awareness – operational, business, and clinical impacts
- ❑ **Establish a cadence and process for coordination with IT/IS and Cybersecurity**
  - Consider Command Center coordination or unified command based on organizational structure (Hospital, IT/IS, and Cybersecurity Command)
- ❑ **Activate applicable continuity and downtime plan(s)**
  - Review current business continuity and downtime plans and make adjustments or updates to meet the cyber incident scenario as needed
- ❑ **Communicate activation of downtime plans to inform operational changes**
  - Consider use of overhead paging, mass notification system, etc.
  - In some cases, traditional communications may not be available and notification will need to be made via non-traditional methods
  - Consider the use of non-traditional communication methods as typical communication methods may be impacted.
- ❑ **Approve recommendations from Operations relative to**
  - Scaling patient care, operational or administrative services
  - Pausing patient care, operational or administrative services
  - Initiating diversionary status
- ❑ **Address cyber incident need by activating additional resources**
- ❑ **Understand upstream and downstream impact(s) to partner organizations. Communicate as appropriate.**
  - Community Connect
  - Other health systems
  - Community partners (e.g., Skilled Nursing Facilities, Long-term Acute Care, Emergency Medical Services)
- ❑ **Consider notification to internal or contracted legal teams**
  - Seek guidance on federal and state regulatory or other requirements
  - Request assistance navigating insurance notification and coverage
  - Leverage support with law enforcement notification and involvement
- ❑ **Establish cadence for ongoing impact assessment and briefing (e.g., operational periods)**

Medical-Technical Specialist (Subject Matter Expert/Advisor)

Role: Subject matter expert(s) who advises the Incident Commander or Section Chief on issues related to response; provides understanding and communicates specific impact and recommendations given their area of expertise.

Given the complexity and scope of this response, it is recommended to activate a Medical Technical Specialist Team. This could alternatively be activated as a branch within Information Technology / Systems Section Chief.

- ❑ **Cybersecurity**
  - Collaborate with IT/IS to contain the spread of malicious activity
  - Perform analysis and forensics as needed to isolate the threat
  - Identify impacted systems – consider Clinical Engineering, Lab, Pharmacy, Imaging, etc.
  - Request additional expertise based on capability of internal team
  - Engage third-party / outside cybersecurity vendor to support cyber incident response activities
- ❑ **Chief Nursing Officer/Chief Medical Officer/Clinical Leader/Safety & Quality**
  - Advise on issues with ethical implications
  - Understand and communicate clinical impact(s) to inform waivers, contingency care or Crisis Standards of Care activation
  - Coordinate with Medical Staff Office, Transfer Center, and Telehealth Services for needs relative to rapid credentialing, privileging, and reduction/expansion of services
  - Consider special populations, including pediatrics, transplant, behavioral medicine, etc.
- ❑ **Risk Management/Regulatory & Compliance/Legal**
  - Evaluate the incident's short term and long term impacts and provide guidance to the incident commander on potential modifications required for risk management and loss prevention program policies
  - Consider activation of Cyber Insurance policy and procedures
  - Consider extortion components
  - Consider initiation of digital forensics/incident response (DFIR)
  - Gather invoices to support non-cyber-related claim file process
  - Complete other reporting requirements
  - Provide notification to regulatory agencies as appropriate
- ❑ **Privacy Officer/Privacy Department**
  - Provide information and guidance on the potential of a breach of sensitive information due to the cybersecurity incident; this could include but not limited to PHI, PCI, PII, etc. breaches.
  - Provide guidance on necessary notification and regulatory actions associated with privacy breaches.
  - Partner with legal stakeholders to initiate necessary privacy notifications.

Public Information Officer

Role: Serve as the conduit for information to internal and external stakeholders, including site personnel, visitors and families, and the news media, as approved by Cybersecurity, IT/IS Section Chief and the Incident Commander.

- ❑ **Receive briefing from Incident Commander on situation and status**
- ❑ **Establish cadence for coordination with Cybersecurity leadership or other Med-Tech Specialist for collaboration on internal and external communications**
- ❑ **If appropriate, activate crisis communication plan**[5]
- ❑ **Rapidly develop internal communication for approval by Incident Commander**
  - Identify an internal spokesperson and provide guidance as appropriate
  - Establish a plan to communicate to current and incoming staff
    - Recommend operations section leverage local leaders for local guidance
    - Include providers in scope of communication

  Note: Consider that internal communication rapidly becomes external
  - Develop talking points for staff in patient or public facing departments

  Note: this should include phone-related services
  - Identify a mechanism and cadence for executive communication
    - Consider communication to executives/ board of trustees
    - Hospital leadership notification (may depend on size and scope of facility)
- ❑ **Collaborate with Operations Section Chief and IT/IS Section Chief to support activation of redundant communications, if available**
  - If needed, collect contact information for Command and general staff and create communication directory
  - Distribute paper directory with Command and general staff contact information
- ❑ **Develop cyber incident resources for patients, family members, and community members**
  - Coordinate with Liaison role and Cybersecurity SME on appropriate notification to approved partner(s)
  - Incident Commander to review and approve all internal and external communications
  - Consider alternate phone numbers to contact site services
  - Consider access to online records or teleservices
  - Consider the impact to internal Wi-Fi connectivity
  - Consider family members of onsite staff
- ❑ **Collaborate with Operations Section Chief to develop and provide messaging to neighboring hospitals of impacted operations, diversion plans, suspension of services, etc.**
- ❑ **Collaborate with Cybersecurity and Legal Department to develop a media and PR strategy**

  Note: During a cybersecurity incident, **providing information to the public may create additional vulnerabilities.** If a criminal investigation is possible, coordination with law enforcement will be required to identify what details may be disclosed. Depending on law enforcement cybersecurity investigation guidance, notification could include local, state, tribal and /or FBI law enforcement agencies.
  - Identify the scope of information that can be shared and to what audience
  - Monitor social media and other media reports
  - Identify if and how information may be provided to media outlets
  - Consider notifying security partners/ information sharing organizations to prevent further compromises of the health sector

5 https://emergency.cdc.gov/cerc/ppt/CERC_Crisis_Communication_Plans.pdf

Liaison

Role: Function as the cyber incident contact for the Command Center for representatives from federal, state or local agencies.

- ❑ **Coordinate external partner communication with Public Information Officer, Med-Tech, IT/IS Section Chief**

  Note: if not activating Med-Tech Section, ensure coordination with Cybersecurity

- ❑ **Provide notifications and updates to regulatory organizations as required. Considerations include:**
  - Emergency Medical Service (EMS)
  - Local and state dispatch centers
  - Municipal Emergency Management
  - Government Agencies
  - Health Department
  - Healthcare Coalition
- ❑ **Identify and support the potential need for a Unified Command structure**

Safety Officer

Role: Identify, monitor, and mitigate safety risks to patients, staff, and visitors during a prolonged large-scale outage.

- ❑ **Understand and address safety impacts based on cyber incident. These may include:**
  - Central and remote patient monitoring
  - Telehealth services
  - Duress/Distress/panic alarm/nurse call alerting buttons or systems
  - Imaging
    - Readability
    - Integrity
  - Pharmacy
    - Dispensing
    - Automated safety checks
  - Environmental controls
    - Refrigeration
    - Temperature tracking
    - Sterile processing
    - Heating, Ventilation, and Air Conditioning
    - Humidity
    - Air exchange
    - Pressure
  - Access control systems:
    - Physical access and closed-circuit television
    - Card Access Readers
    - Infant Protection Systems
  - Other network-reliant systems
    - Tube system
    - Lab devices
    - Mass communication (e.g., text paging, overhead paging, radio repeaters)
  - Mechanism for safety reporting
    - Patient
    - Employee
    - Visitor
- ❑ **Utilize Physical Access Control Processes**
  - All external response partners / agencies should be directed to the Command Center or other location identified by the Incident Commander
  - Validate identification of any entities and individuals entering the facility during a cyber incident
  - Capture a record of all external stakeholders who enter the facility

Operations Section Chief

Role: Develop and recommend strategies and tactics to continue clinical and non-clinical operations for the duration of the cyber incident response and for recovery.

- ❑ **Activate downtime procedures**
  - Identify safe, alternative processes for patient care based on technical outage
  - Initiate downtime processes:
    - Utilize business continuity or downtime computers or other downtime charting modalities
    - Build paper charts for all patients using information printed from downtime computers or paper downtime forms.
    - Print critical service delivery information (e.g., patient charts, staff schedules, patient schedules)
    - Establish patient and specimen label process
    - Identify devices that can be operated in an offline mode and potential limitations

  Note: This could be an extended downtime (days or weeks) with lasting impacts for multiple months – address downtime procedures that need to be refined to support extended downtime
  - Establish or implement back charting criteria
  - Deploy strike teams to provide just-in-time training and regulatory requirements on downtime charting and documentation
  - Request clinical users to triage which technology seems to be available and unavailable and report back to the Hospital Incident Command System (HICS) structure
- ❑ **Activate business continuity plans for clinical and operational services**
- ❑ **Conduct ongoing assessment of impacts to patients, staff, space, supplies, and equipment across different care areas**
  - ED/Trauma
  - Critical Care
  - Acute Care
  - Women's & Newborn
  - Surgical Services
  - Pediatric Care
  - Air medical services
  - Telehealth
  - Transfer Center
  - Behavioral Health
  - Oncology
  - Transplant
  - Staffing needs
- ❑ **Provide recommendations for scaling back services**
  - Non-urgent elective procedures
  - Outpatient services
  - Provide recommendations for alternate sites of care
    - Oncology/Radiation
    - Dialysis
    - Infusion Care
- ❑ **Provide recommendations for delaying services**
  - Non-urgent elective procedures
  - Outpatient services
- ❑ **Provide recommendations for altering**
  - Laboratory Services (e.g., test volumes, specimen processing, outsourcing)
  - Imaging Services (e.g., time-sensitive or emergent only)
  - Pharmacy Services (e.g., decrease outpatient services)
  - Rehabilitative Services
- ❑ **Consider and communicate the need for staff resiliency resources (Employee Assistance Program, mental health, etc.) for extended cyber incident support**

Planning Section Chief

Role: Oversee all cyber incident related documentation regarding cyber incident operations and resource management; initiate long range planning; conduct planning meetings; prepare the Incident Action Plan (IAP) for each operational period.

- ❑ **In collaboration with the Incident Commander, use the planning tool, the Planning P to**
  - Establish operational periods
  - Record cyber incident objectives
  - Develop Incident Action Plan (IAP)
  - Schedule and execute appropriate briefings and reviews
- ❑ **Collect status report and escalation from different departments**
  - Prioritize critical areas and needs
- ❑ **Develop situation-report for command staff**
- ❑ **Contact local area leaders who did not report status**
- ❑ **Prepare for patient and personnel tracking in digital and printed form**
  - Patient logs
  - Staffing logs
- ❑ **Develop a timeline of events that can be used to track cyber incident response actions and support retroactive review of actions and timelines**
  - Implementation of action items
  - Notable actions
  - Incident milestones
  - Incident decisions
- ❑ **Prepare staffing plan and recommendations to support operations**
  - Support staff may be needed to support the outage – engage staffing office
    - Consider experienced staff/champions skilled in downtime procedures
  - Consider extended needs which may require:
    - Runners
    - Transporters
    - Nursing ratios
    - Redeployment
    - Remote work: continuation vs. site needs
    - Onsite support: loss of telehealth or other services
    - Engaging Liaison section for external resource support
- ❑ **In collaboration with Operations Section Chief and Public Information Officer, develop process for contacting patients and their family members regarding alterations to procedures and appointments**

Finance Section Chief

Role: Monitor the utilization of financial assets and the accounting for financial expenditures; supervise the documentation of expenditures and cost reimbursement activities.

- ❑ **Track costs, expenditures, and revenue impacts**
- ❑ **Develop contingency strategies for impacts to financial data**
  - Engage appropriate section chief(s) to communicate changes
- ❑ **Consider establishing a cost center specific to the cyber incident**
- ❑ **Gather invoices to support non-cyber-related claim file processes**
- ❑ **Consider modifying restrictions for purchase card or corporate card limits**
- ❑ **Develop and communicate contingency strategies for impacts to retail or point-of-sale systems**
- ❑ **Facilitate contracting for other emergency support as needed**
- ❑ **Oversee manual payroll and timekeeping processes as needed**
- ❑ **Coordinate with outside vendors for delayed or manual payment processes**
- ❑ **Partner with the SMEs outlined in the Med-Tech section on insurance and reimbursement documentation**

Logistics Section Chief

Role: Organize and direct the service and support activities needed to ensure material needs for the site's response to a cyber incident are available when needed.

- ❑ **Identify any potential disruptions to critical infrastructure and priority services**
- ❑ **Regularly evaluate electrical system performance**
  - Consider network-reliant systems (e.g., tube system, temperature controls, etc.)
  - Deploy additional staff to manually monitor systems reliant on the network (HVAC, humidity, etc.)
  - If the fire suppression system is reliant on the technical network, activate a fire watch
- ❑ **Partner with IT/IS to identify communication redundancies for**
  - Translation services (services offered previously via telehealth may need to be brought on site)
  - Visitors, family members, clergy, or vendors (e.g., phone or video calls, end of life care)
- ❑ **Ensure food and hydration is available; consider patients, staff, visitors, and Command Center personnel**
- ❑ **Prepare for radio deployment**
  - Ensure radios are charged and there is a plan for additional batteries as needed
  - Provide just-in-time training on radio use
  - Oversee sign-out sheet to track all deployed radios
- ❑ **Ensure adequate downtime supplies: paper, toner, pencils, pens, stationary, forms, etc.**
- ❑ **Order additional supplies as needed**
- ❑ **Assess impacts to materials management and ordering processes**
  - Implement manual inventory and ordering processes for supply chain management
  - Implement a manual process for distribution, supply chain, and redistribution of clinical and operational supplies
  - Ensure availability of durable medical equipment
  - Ensure availability of oxygen
  - Ensure availability of pharmaceuticals
- ❑ **Deploy Environment of Care teams to evaluate contingency needs**
  - Clinical Engineering/Health Technology Management
  - Environmental Services
  - Facilities/Maintenance/Engineering
  - Industrial Hygiene
  - Infection Prevention
  - Physical Security
- ❑ **Assess ability to source additional technical equipment for end users (laptops, tablets, etc.)**
- ❑ **Redeploy excess staff to support operations**
- ❑ **Establish labor pool or coordinated process to redeploy staff**

  Note: Credentials and competency must be accounted for
  - Provide instructions for manual timekeeping
  - Identify staff resiliency resources (EAP, mental health, etc.) for extended cyber incident support

Information Technologies (IT) / Information Systems (IS) Section Chief

Role: Provide technical response, continuity, and recovery recommendations; partner with cybersecurity to inform cyber incident response decisions and activities. Coordinates intelligence and investigation efforts.

Note: This role should be filled with IT/IS professionals.

If using an Internal Unified Command Structure, consider removing the Cybersecurity section from the Med-Tech role and place within this role.

- ❑ **Address potential IT/IS/Cybersecurity staffing needs and establish staff rotation schedule**
- ❑ **Address any qualifications or security clearance necessary based on cyber incident complexity**
- ❑ **Triage the impact of the cyber incident to identify segmented or usable services or applications**
- ❑ **Establish a cadence with cybersecurity for regular situation updates to inform Command**
  - Communicate scope and severity of disruption
  - Identify and communicate upstream and downstream impacts
  - Support identification and implementation of safe, alternate processes
  - Assist with restoration of technology systems
- ❑ **Identify opportunities that limit the spread of the cyber incident. If possible:**
  - Segment or isolate servers
  - Provide guidance on how to disconnect the data center from your environment
  - Quarantine or sever the connection with data centers to limit spread
- ❑ **Coordinate with internal and/or external Clinical Engineering/Health Technology Management to understand**
  - Impacts
  - Data storage limits to inform downtime processes
- ❑ **Collaborate with Cybersecurity to understand scope of disruption and potential impact of cyber incident**
- ❑ **Consider activating unified command with a cyber command structure**
  - Activate cyber insurance policy and procedures
  - Coordinate legal and risk management activities
- ❑ **Identify the impact on the following systems**
  - Bedside care: monitoring, telemetry, pumps, nurse call
  - Building systems (e.g., tube system, temperature tracking, badge access)
  - Electronic health record
  - Emergency Department/ Trauma Services
  - Imaging
  - Internet
  - Intranet
  - IS Infrastructure
  - Lab
  - Network
  - Revenue Cycle
  - Surgical Services
  - Remote work capabilities
  - Telecom

- ❑ **Establish Labor Pool or coordinated process to redeploy staff**
  Note: Credentials and competency must be accounted for
  - Provide instructions for manual timekeeping
- ❑ **At direction of CISO or Cybersecurity leader, consider proactive technical system(s) lockdown**
  - Consider data center shutdown to prohibit spread
  - Consider critical systems shutdown to limit unauthorized access to data and records
  - Consider shutdown of vendor bi-directional VPN access
  - Consider shutdown of WAN connections
  - Consider lockdown of internal network segments
  - Consider failover to Disaster Recovery, quarantine routers/switches
  - Scan all backups for integrity
- ❑ **Consider a recommendation to power down all technology to limit the spread**
  - Engage IT/IS to support network take down/recovery
  - Engage IT/IS in use of off-network computers for downtime process support
- ❑ **Establish a process for interim solution, intake, and prioritization**
- ❑ **Identify Recovery Time Objective (RTO) / Recovery Point Objective (RPO) for essential services and applications and if possible, leverage failover options or implement disaster recovery as soon as possible.**
- ❑ **Provide updates to Command staff on estimated length of time until systems can be fully recovered (RTO/RPO in hours/days/weeks)**
- ❑ **Coordinate with Cybersecurity on timeline for threat eradication**
  Note: Re-enabling internet/WAN/VPNs may not be possible until threat is eradicated
- ❑ **Collaborate with Operations Section Chief to start a recovery plan for essential services and applications**
- ❑ **Collaborate with Incident Command on restoration and recovery processes**
  Note: This guide is for the first 12 hours; however, recovery should begin immediately
  - Identify scope of encryption
  - Reaffirm recovery time objectives
  - Validate critical application recovery priority
  - Assess critical application dependencies for recovery
  - Recover critical applications for essential business operations in a timely manner
  - Recover infrastructure

Appendix

Original Publication Acknowledgments

This Operational Continuity-Cyber Incident (OCCI) checklist was developed by the Healthcare and Public Health Sector Coordinating Council (HSCC). It represents the best collective thinking of private-sector cybersecurity and emergency management executives of the HSCC Incident Response/Business Continuity (IRBC) Task Group of the Health Sector Coordinating Council's Cybersecurity Working Group (CWG).

HHS would like to thank all HSCC IRBC Task Group members who collectively dedicated thousands of hours of their valuable time and expertise to develop the OCCI checklist. HHS also extends special thanks to the following authors and members of the original publication for their contributions to this document.

Garrett Hagood
Kirsten Nunez
Mike Caudill
Nate Couture
Hazel Chappel
Lisa Bisterfeldt
Mitch Parker
Skip Skivington

Revised Publication Acknowledgments

In early 2023, the HSCC and IRBC requested the 405(d) Program and Task Group fold the Healthcare and Public Health Sector Coordinating Council (HSCC) document, the Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR), into the 405(d) family of publications. The 405(d) Task Group created a sub-working group to review the original publication, add content, and aligned the document with the 405(d) Program mission and vision. This edition is the result of the leadership and the collaboration of the following groups and professionals: the HPH Joint Cybersecurity Working Group, the Health Sector Coordinating Council, the Population Health Information Sharing and Analysis Center (PH-ISAC), the 405(d) Steering Committee, and the 405(d) Task Group.

The department would like to thank the members of the 405(d) Task Group for their time and knowledge leveraged in improving the content, maturity, and functionality of the Operational Continuity-Cyber Security Checklist. HHS would like to mention the leadership and collaboration of the following professionals:

Lisa Bisterfeldt
Kirsten Nunez
Nathan Couture
Chris Murray
Lee Barrett
Ashley Eng
Kevin Scott
Hazel Chappell
Oleg Yusim
Kimberly Ann Bauer
Brindusa Curcaneanu
Edward Marchewka
Jaz-Michael King
Jeff Bontsas
Zack Gable
Mark Jarrett
Ronald Mehring
David Sims
John Matusiak
Andrew Sargent
Steven Hughes
Jim Swanson
John Litzenberg
Ed Gaudet
Jason Taule
Mark Baik
Michael Johnston
Stacey Bradley
Robert Rajewski
Reuven Pasternak
Mike Caudill
Bill McDonald

The 405(d) Program would also like to express gratitude to HHS, DHS, and NIST for their input, collaboration, and efforts to establish and support the 405(d) Task Group and the updated edition.

Importance of Reporting Cyber Incidents

HPH entities are strongly encouraged to report cyber incidents to the Federal Government as soon possible, especially if they believe the newly discovered cybersecurity incident may pose a risk to national security or public safety. This early outreach allows for the timely collection of the facts and circumstances of the incident which might help accelerate the identification of tactics, techniques, and procedures (TTPs) used in the incident, accelerate the recovery process and also prevent other entities from becoming the victims. Here is some information about reporting cyber incidents to the Federal Government:

Report cybercrime, including computer intrusions or incidents, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI:

Federal Bureau of Investigation (FBI) FBI Field Office Cyber Task Forces

Internet Crime Complaint Center (IC3)

National Cyber Investigative Joint Task Force NCIJTF CyWatch 24/7 Command Center or (855) 292-3937

Report Cyber Incidents to the Cybersecurity and Infrastructure Security Agency (CISA)

On December 18, 2023, The Securities and Exchange Commission established new requirements for companies to disclose material cybersecurity incidents. The FBI, in coordination with the Department of Justice, is providing guidance on how victims can request disclosure delays for national security or public safety reasons. The FBI recommends all publicly traded companies establish a relationship with the cyber squad at their local FBI field office. For more information regarding this requirement, please refer to FBI Guidance to Victims of Cyber Incidents on SEC Reporting Requirements.

General questions regarding HPH cybersecurity should be directed to HHS via email to: hhscyber@hhs.gov.

HHS as the Sector Risk Management Agency for Healthcare and Public Health (HPH)

Critical Infrastructure are those assets, systems, and networks that provide functions necessary for our way of life. There are 16 critical infrastructure sectors that are part of a complex, interconnected ecosystem and any threat to these sectors could have potentially debilitating national security, economic, and public health or safety consequences. In 2021, Congress codified and formalized the role of Sector Risk Management Agencies (SRMA), which were previously specified in other guidance[5]. Section 9002(b) of the National Defense Authorization Act (NDAA), outlines responsibilities and expectations for SRMAs, to include facilitating information sharing, performing sector coordination, supporting incident management, and contributing to emergency preparedness efforts. HHS has been designated as the SRMA for the Healthcare and Public Health (HPH) Sector.

Additional legislation outlining HHS's role in supporting HPH sector cybersecurity is the Cybersecurity Act of 2015. Within this legislation is Section 405(d): Aligning Healthcare Industry Security Approaches. In response to the CSA Section 405(d) requirement, HHS leveraged the HPH Sector's Critical Infrastructure Security and Resilience Partnership to establish the 405(d) Task Group. HHS convened the Task Group in 2017 to develop vetted cybersecurity resources based on industry best practices. In 2018, the first version of Health Industry Cybersecurity Practices (HICP), was released and an updated version was released in 2023. The updated version included topics such as Defense in Depth and Zero Trust. The OCCI document will be the latest joint publication released between the government and industry.

In January 2024 HHS released the voluntary Healthcare and Public Health Cybersecurity Performance Goals (HPH CPGs), aligned with the department's overall cyber strategy. Among other things, these HPH CPGs emphasize the importance of incident planning and preparedness activities, to include encouraging organizations to consistently maintain, drill, and update cybersecurity incident response plans for relevant threat scenarios. HHS has numerous cybersecurity resources that can support HPH entities in enhancing their cyber resilience. These resources are developed by divisions across HHS—often jointly with industry—and include best practice guidance such as those mentioned previously, education, threat specific intelligence, and more. HHS recently launched a new gateway website as part of its efforts to establish a one-stop-shop for HHS cyber and simplify how the sector can access HHS resources and tools across all HHS divisions.

The Administration for Strategic Preparedness and Response (ASPR) leads the HHS SRMA Cybersecurity Working Group (CWG) as the department's primary mechanism to coordinate its statutory responsibility as the HPH SRMA. The CWG is the body that coordinates and collaborates across the HHS cyber community to identify cyber threats to the sector, coordinates across HHS divisions to prepare for and mitigate potential or identified cyber incidents, shares information, and coordinates policy recommendations, resources, and messaging to strengthen and build cyber resiliency within the HPH sector. Check out a diagram which further explains the role that each partner plays on the HHS #Cyber Team, as outlined in the department's recent cyber strategy.

5 Pub. L. 116-283, § 9002(c), William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 116th Congress, January 1, 2021, https://www.congress.gov/bill/116th-congress/house-bill/6395.

HHS #Cyber Team

HHS works as a team to help the Healthcare and Public Health (HPH) sector prepare for and respond to cyber threats. Cyber Safety is Patient Safety!

The Advanced Research Projects Agency for Health (ARPA-H) launched the Digital Health Security (DIGIHEALS) project to ensure patients continue to receive care in the wake of a medical facility cyberattack.

The Health Sector Cybersecurity Coordination Center (HC3) enriches and analyzes cyber security threat information to develop objective mitigations for and in collaboration with the health and public health sector. HC3 achieves this through directed engagements, action based alerts, and public threat briefings.

The HHS 405(d) Program is a collaborative effort between the Health Sector Coordinating Council and the federal government to align healthcare industry security approaches by providing useful HPH-focused resources to help educate, raise awareness, and drive behavioral change.

The Office of the National Coordinator for Health Information Technology (ONC) in the HHS Office of the Secretary, is a resource to the entire health system to support the adoption of health information technology and the promotion of nationwide, standards-based health information exchange to improve healthcare, including information privacy and security.

ASPR

The Administration for Strategic Preparedness and Response's (ASPR) coordinates all HHS cybersecurity support and leads external collaboration in its role as the Sector Risk Management Agency (SRMA) on behalf of HHS for the Healthcare and Public Health (HPH) sector.

The Office of National Security (ONS) conducts all-source intelligence analysis to inform HHS policy and drive operational planning activities. ONS executes its mission, through departmental and Intelligence Community coordination, by providing timely and relevant threat intelligence to HHS senior leaders and staff involved in executing the HPH SRMA mission.

The Centers for Medicare & Medicaid Services (CMS) protects and controls the confidentiality, integrity, and availability of CMS information and information systems. CMS also works to promote cybersecurity and safe care in response to cyber threats across its programs, including Medicare, Medicaid, the Children's Health Insurance Program, and the Health Insurance Marketplaces.

The Office for Civil Rights (OCR) administers and enforces the HIPAA Privacy, Security, and Breach Notification Rules through investigations, rulemaking, guidance, and outreach. The HIPAA Rules establish rights for individuals to their protected health information (PHI), requirements for HIPAA regulated entities on uses and disclosures of PHI, and privacy and security protections of PHI. OCR supports improved cybersecurity through cybersecurity investigations resolved with technical assistance, corrective action plans, or civil money penalties and by publishing cybersecurity resources for regulated entities and consumers through guidance, bulletins, newsletters, videos, and applications.

The Food and Drug Administration (FDA) informs patients, healthcare providers and facility staff, and manufacturers about cybersecurity vulnerabilities for connected medical devices and requires that medical devices meet specific cybersecurity guidelines.

CWG

The HHS SRMA Cybersecurity Working Group (CWG) is the primary mechanism used to coordinate HHS's execution of its statutory responsibility as the HPH SRMA. The CWG is the body that coordinates and collaborates across the HHS cyber community to identify cyber threats to the HPH sector, coordinates across HHS divisions to prepare for and mitigate potential or identified cyber incidents, shares information, and coordinates policy recommendations and messaging to strengthen and build resiliency within the HPH sector against cyber threats.

Glossary

Business Continuity Plans - The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

Command Center - Any place that is used to provide centralized command for some purpose.

Community Connect - Typically refers to a healthcare initiative or program designed to improve healthcare access, coordination, and communication between healthcare organizations and the communities they serve. Community Connect programs aim to bridge the gap between healthcare providers and the broader community by fostering collaboration and engagement.

Critical Infrastructure - System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Cyber Incident - Actions taken through the use of an information system or network that jeopardizes the confidentiality, integrity, or availability or potentially causes adverse effects on information system(s), network(s), and/or the information residing therein.

Environment of Care (EOC): Are teams that are multidisciplinary groups within healthcare organizations responsible for ensuring a safe and compliant physical environment for patients, visitors, and staff. The EOC teams play a crucial role in managing and monitoring various aspects of the healthcare facility to maintain a safe and functional environment.

Development Cycle (Development Life Cycle) - The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

Digital Forensics - The process used to acquire, preserve, analyze, and report on evidence using scientific methods that are demonstrably reliable, accurate, and repeatable such that it may be used in judicial proceedings.

Incident Command Activation - In the context of an Incident Response Plan (IRP) for a cyber incident, refers to the process of formally initiating and organizing the response efforts when a cybersecurity incident occurs. It involves establishing a structured command hierarchy to effectively manage and coordinate the response to the incident.

Recovery Point Objective (RPO) - The maximum amount of data that can be lost after recovering from a cyber incident before exceeding what is acceptable to an organization.

Recovery Time Objective (RTO) - The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes.

Security Incident - 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.

Incident Commander

ROLE

Provides overall strategic direction on all site-specific response actions and activities.

- ❑ **Formal declaration of an incident**
  - Define size and scale of command activation
  - Define type of command (in person, virtual, single, multiple)
  - Define communication modalities based on incident
- ❑ **Identify incident scope and obtain situational awareness**
  - Identify Scope – One site/multiple sites/isolated outage/full network outage
  - Assume it is a malicious cybersecurity incident until proven otherwise
  - Situational awareness – operational, business, and clinical impacts
- ❑ **Establish a cadence and process for coordination with IT/IS and Cybersecurity**
  - Consider Command Center coordination or unified command based on organizational structure (Hospital, IS/IT, and Cybersecurity Command)
- ❑ **Activate applicable continuity and downtime plan(s)**
  - Review current continuity and downtime plans and make adjustments or updates to meet the incident scenario as needed
- ❑ **Communicate activation of downtime plans to inform operational changes**
  - Consider use of overhead paging, mass notification system, etc.
  - In some cases, traditional communications may not be available and notification will need to be made via non-traditional methods
  - Consider the use of non-traditional communication methods as typical communication methods may be impacted.
- ❑ **Approve recommendations from Operations relative to**
  - Scaling patient care, operational or administrative services
  - Pausing patient care, operational or administrative services
  - Initiating diversionary status
- ❑ **Address incident need by activating additional resources**
- ❑ **Understand upstream and downstream impact(s) to partner organizations.**
  Communicate as appropriate.
  - Community Connect
  - Other health systems
  - Community partners (e.g., Skilled Nursing Facilities, Long-term Acute Care, Emergency Medical Services)
- ❑ **Consider notification to internal or contracted legal teams**
  - Seek guidance on federal and state regulatory or other requirements
  - Request assistance navigating insurance notification and coverage
  - Leverage support with law enforcement notification and involvement
- ❑ **Establish cadence for ongoing impact assessment and briefing (e.g., operational periods)**

To learn more about how you and your organization can prepare for a cyber event, check out the Operational Continuity-Cyber Incident (OCCI) Checklist. Be sure to check out the other available resources HHS has to offer at the Healthcare and Public Health Cybersecurity Gateway at hhscyber.hhs.gov as well as 405(d) specific resources at 405d.hhs.gov and our 405(d) social media pages: @ask405d on Facebook, X, LinkedIn, and Instagram!

Medical-Technical Specialist (Subject Matter Expert/Advisor)

ROLE

Subject matter expert(s) who advises the Incident Commander or Section Chief on issues related to response; provides understanding and communicates specific impact and recommendations given their area of expertise.

Given the complexity and scope of this response, it is recommended to activate a Medical Technical Specialist Team. This could alternatively be activated as a branch within Information Technology / Systems Section Chief.

❑ Cybersecurity

- Collaborate with IT/IS to contain the spread of malicious activity
- Perform analysis and forensics as needed to isolate the threat
- Identify impacted systems – consider Clinical Engineering, Lab, Pharmacy, Imaging, etc.
- Request additional expertise based on capability of internal team
- Engage third-party / outside cybersecurity vendor to support incident response activities

❑ Chief Nursing Officer/Chief Medical Officer/Clinical Leader/Safety & Quality

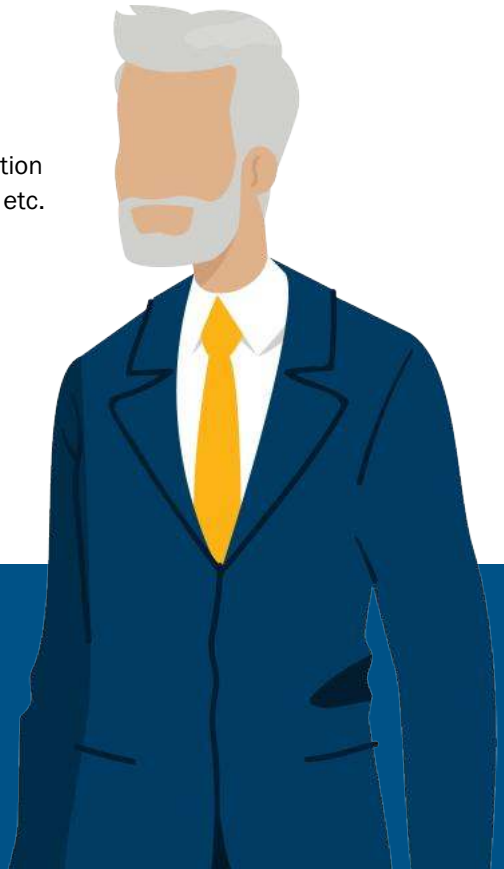
- Advise on issues with ethical implications
- Understand and communicate clinical impact(s) to inform waivers, contingency care or Crisis Standards of Care activation
- Coordinate with Medical Staff Office, Transfer Center, and Telehealth Services for needs relative to rapid credentialing, privileging, and reduction/expansion of services
- Consider special populations, including pediatrics, transplant, behavioral medicine, etc.

❑ Risk Management/Regulatory & Compliance/Legal

- Evaluate the incident's short and long term impacts and provide guidance to the incident commander on potential modifications required for risk management and loss prevention program policies
- Consider activation of Cyber Insurance policy and procedures
- Consider extortion components
- Consider initiation of digital forensics/incident response (DFIR)
- Gather invoices to support non-cyber-related claim file process
- Complete other reporting requirements
- Provide notification to regulatory agencies as appropriate

❑ Privacy Officer/Privacy Department

- Provide information and guidance on the potential of a breach of sensitive information due to the cybersecurity incident; this could include but not limited to PHI, PCI, PII, etc. breaches.
- Provide guidance on necessary notification and regulatory actions associated with privacy breaches.
- Partner with legal stakeholders to initiate necessary privacy notifications.



To learn more about how you and your organization can prepare for a cyber event, check out the Operational Continuity-Cyber Incident (OCCI) Checklist. Be sure to check out the other available resources HHS has to offer at the Healthcare and Public Health Cybersecurity Gateway at hhscyber.hhs.gov as well as 405(d) specific resources at 405d.hhs.gov and our 405(d) social media pages: @ask405d on Facebook, X, LinkedIn, and Instagram!

Public Information Officer

ROLE

Serve as the conduit for information to internal and external stakeholders, including site personnel, visitors and families, and the news media, as approved by Cybersecurity, IS/IT Section Chief and the Incident Commander.

- ❑ **Receive briefing from Incident Commander on situation and status**
- ❑ **Establish cadence for coordination with Cybersecurity leadership or Med-Tech Specialist for collaboration on internal and external communications**
- ❑ **If appropriate, activate crisis communication plan**[1]
- ❑ **Rapidly develop internal communication for approval by Incident Commander**
  - Identify an internal spokesperson and provide guidance as appropriate
  - Establish a plan to communicate to current and incoming staff
    - Recommend operations section leverage local leaders for local guidance
    - Include providers in scope of communication

  Note: Consider that internal communication rapidly becomes external
  - Develop talking points for staff in patient or public facing departments

  Note: this should include phone-related services
  - Identify a mechanism and cadence for executive communication
    - Consider communication to executives/board of trustees
    - Hospital leadership notification (may depend on size and scope of facility)
- ❑ **Collaborate with Operations Section Chief and IT/IS Section Chief to support activation of redundant communications, if available**
  - If needed, collect contact information for Command and general staff and create communication directory
  - Distribute paper directory with Command and general staff contact information.
- ❑ **Develop incident resources for patients, family members, and community members**
  - Coordinate with Liaison role and Cybersecurity SME on appropriate notification to approved partner(s)
  - Incident Commander to review and approve all internal and external communications
  - Consider alternate phone numbers to contact site services
  - Consider access to online records or teleservices
  - Consider the impact to internal Wi-Fi connectivity
  - Consider family members of onsite staff
- ❑ **Collaborate with Operations Section Chief to develop and provide messaging to neighboring hospitals of impacted operations, diversion plans, suspension of services, etc.**
- ❑ **Collaborate with Cybersecurity and Legal Department to develop a media and PR strategy**

  Note: During a cybersecurity incident, **providing information to the public may create additional vulnerabilities.** If a criminal investigation is possible, coordination with law enforcement will be required to identify what details may be disclosed. Depending on law enforcement cybersecurity investigation guidance, notification could include local, state, tribal and /or FBI law enforcement agencies.
  - Identify the scope of information that can be shared and to what audience
  - Monitor social media and other media reports
  - Identify if and how information may be provided to media outlets
  - Consider notifying security partners/ information sharing organizations to prevent further compromises of the health sector

1 https://emergency.cdc.gov/cerc/ppt/CERC_Crisis_Communication_Plans.pdf

To learn more about how you and your organization can prepare for a cyber event, check out the Operational Continuity-Cyber Incident (OCCI) Checklist. Be sure to check out the other available resources HHS has to offer at the Healthcare and Public Health Cybersecurity Gateway at hhscyber.hhs.gov as well as 405(d) specific resources at 405d.hhs.gov and our 405(d) social media pages: @ask405d on Facebook, X, LinkedIn, and Instagram!

Liaison

ROLE

Function as the incident contact for the Command Center for representatives from federal, state or local agencies.

- ❑ **Coordinate external partner communication with Public Information Officer, Med-Tech, IT/IS Section Chief**

  Note: if not activating Med-Tech Section, ensure coordination with Cybersecurity

- ❑ **Provide notifications and updates to regulatory organizations as required. Considerations include:**
  - Emergency Medical Service (EMS)
  - Local and state dispatch centers
  - Municipal Emergency Management
  - Government Agencies
  - Health Department
  - Healthcare Coalition
- ❑ **Identify and support the potential need for a Unified Command structure**

To learn more about how you and your organization can prepare for a cyber event, check out the Operational Continuity-Cyber Incident (OCCI) Checklist. Be sure to check out the other available resources HHS has to offer at the Healthcare and Public Health Cybersecurity Gateway at hhscyber.hhs.gov as well as 405(d) specific resources at 405d.hhs.gov and our 405(d) social media pages: @ask405d on Facebook, X, LinkedIn, and Instagram!

Safety Officer

ROLE

Identify, monitor, and mitigate safety risks to patients, staff, and visitors during a prolonged large-scale outage.

❑ Understand and address safety impacts based on cyber incident. These may include:

- Central and remote patient monitoring
- Telehealth services
- Duress/Distress/panic alarm/nurse call alerting buttons or systems
- Imaging
  - Readability
  - Integrity
- Pharmacy
  - Dispensing
  - Automated safety checks
- Environmental controls
  - Refrigeration
  - Temperature tracking
  - Sterile processing
  - Heating, Ventilation, and Air Conditioning
  - Humidity
  - Air exchange
  - Pressure
- Access control systems:
  - Physical access and closed-circuit television
  - Card Access Readers
  - Infant Protection Systems
- Other network-reliant systems
  - Tube system
  - Lab devices
  - Mass communication (e.g., text paging, overhead paging, radio repeaters)
- Mechanism for safety reporting
  - Patient
  - Employee
  - Visitor

❑ Utilize Physical Access Control Processes

- All external response partners / agencies should be directed to the Command Center or other location identified by the Incident Commander
- Validate identification of any entities and individuals entering the facility during an incident
- Capture a record of all external stakeholders who enter the facility

To learn more about how you and your organization can prepare for a cyber event, check out the Operational Continuity-Cyber Incident (OCCI) Checklist. Be sure to check out the other available resources HHS has to offer at the Healthcare and Public Health Cybersecurity Gateway at hhscyber.hhs.gov as well as 405(d) specific resources at 405d.hhs.gov and our 405(d) social media pages: @ask405d on Facebook, X, LinkedIn, and Instagram!

Operations Section Chief

ROLE

Develop and recommend strategies and tactics to continue clinical and non-clinical operations for the duration of the incident response and for recovery.

- ❑ **Activate downtime procedures**
  - Identify safe, alternative processes for patient care based on technical outage
  - Initiate downtime processes:
    - Utilize business continuity or downtime computers or other downtime charting modalities
    - Build paper charts for all patients using information printed from downtime computers or paper downtime forms.
    - Print critical service delivery information (e.g., patient charts, staff schedules, patient schedules)
    - Establish patient and specimen label process
    - Identify devices that can be operated in an offline mode and potential limitations

  Note: This could be an extended downtime (days or weeks) with lasting impacts for multiple months – address downtime procedures that need to be refined to support extended downtime
  - Establish or implement back charting criteria
  - Deploy strike teams to provide just-in-time training and regulatory requirements on downtime charting and documentation
  - Request clinical users to triage which technology seems to be available and unavailable and report back to the Hospital Incident Command System (HICS) structure
- ❑ **Activate business continuity plans for clinical and operational services**
- ❑ **Conduct ongoing assessment of impacts to patients, staff, space, supplies, and equipment across different care areas**
  - ED/Trauma
  - Critical Care
  - Acute Care
  - Women's & Newborn
  - Surgical Services
  - Pediatric Care
  - Air medical services
  - Telehealth
  - Transfer Center
  - Behavioral Health
  - Oncology
  - Transplant
  - Staffing needs
- ❑ **Provide recommendations for scaling back services**
  - Non-urgent elective procedures
  - Outpatient services
  - Provide recommendations for alternate sites of care
    - Oncology/Radiation
    - Dialysis
    - Infusion Care
- ❑ **Provide recommendations for delaying services**
  - Non-urgent elective procedures
  - Outpatient services
- ❑ **Provide recommendations for altering**
  - Laboratory Services (e.g., test volumes, specimen processing, outsourcing)
  - Imaging Services (e.g., time-sensitive or emergent only)
  - Pharmacy Services (e.g., decrease outpatient services)
  - Rehabilitative Services
- ❑ **Consider and communicate the need for staff resiliency resources (Employee Assistance Program, mental health, etc.) for extended incident support**

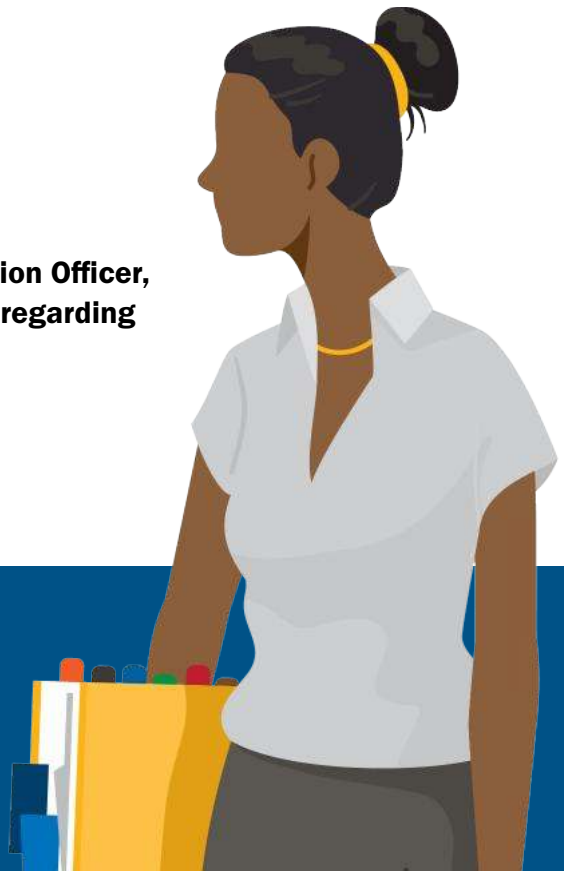
To learn more about how you and your organization can prepare for a cyber event, check out the Operational Continuity-Cyber Incident (OCCI) Checklist. Be sure to check out the other available resources HHS has to offer at the Healthcare and Public Health Cybersecurity Gateway at hhscyber.hhs.gov as well as 405(d) specific resources at 405d.hhs.gov and our 405(d) social media pages: @ask405d on Facebook, X, LinkedIn, and Instagram!

Planning Section Chief

ROLE

Oversee all incident related documentation regarding incident operations and resource management; initiate long range planning; conduct planning meetings; prepare the Incident Action Plan (IAP) for each operational period.

- ❑ **In collaboration with the Incident Commander, use the planning tool, the Planning P to**
  - Establish operational periods
  - Record incident objectives
  - Develop Incident Action Plan (IAP)
  - Schedule and execute appropriate briefings and reviews
- ❑ **Collect status report and escalation from different departments**
  - Prioritize critical areas and needs
- ❑ **Develop situation-report for command staff**
- ❑ **Prepare for patient and personnel tracking in digital and printed form**
  - Patient logs
  - Staffing logs
- ❑ **Develop a timeline of events that can be used to track incident response actions and support retroactive review of actions and timelines.**
  - Implementation of action items
  - Notable actions
  - Incident milestones
  - Incident decisions
- ❑ **Prepare staffing plan and recommendations to support operations**
  - Support staff may be needed to support the outage – engage staffing office
    - Consider experienced staff/champions skilled in downtime procedures
  - Consider extended needs which may require:
    - Runners
    - Transporters
    - Nursing ratios
    - Redeployment
    - Remote work: continuation vs. site needs
    - Onsite support: loss of telehealth or other services
    - Engaging Liaison section for external resource support
- ❑ **In collaboration with Operations Section Chief and Public Information Officer, develop process for contacting patients and their family members regarding alterations to procedures and appointments**



To learn more about how you and your organization can prepare for a cyber event, check out the Operational Continuity-Cyber Incident (OCCI) Checklist. Be sure to check out the other available resources HHS has to offer at the Healthcare and Public Health Cybersecurity Gateway at hhscyber.hhs.gov as well as 405(d) specific resources at 405d.hhs.gov and our 405(d) social media pages: @ask405d on Facebook, X, LinkedIn, and Instagram!

Finance Section Chief

ROLE

Monitor the utilization of financial assets and the accounting for financial expenditures; supervise the documentation of expenditures and cost reimbursement activities.

- ❑ **Track costs, expenditures, and revenue impacts**
- ❑ **Develop contingency strategies for impacts to financial data**
  - Engage appropriate section chief(s) to communicate changes
- ❑ **Consider establishing a cost center specific to the incident**
- ❑ **Gather invoices to support non-cyber-related claim file processes**
- ❑ **Consider modifying restrictions for purchase card or corporate card limits**
- ❑ **Develop and communicate contingency strategies for impacts to retail or point-of-sale systems**
- ❑ **Facilitate contracting for other emergency support as needed**
- ❑ **Oversee manual payroll and timekeeping processes as needed**
- ❑ **Coordinate with outside vendors for delayed or manual payment processes**
- ❑ **Partner with the SMEs outlined in the Med-Tech section on insurance and reimbursement documentation**

To learn more about how you and your organization can prepare for a cyber event, check out the Operational Continuity-Cyber Incident (OCCI) Checklist. Be sure to check out the other available resources HHS has to offer at the Healthcare and Public Health Cybersecurity Gateway at hhscyber.hhs.gov as well as 405(d) specific resources at 405d.hhs.gov and our 405(d) social media pages: @ask405d on Facebook, X, LinkedIn, and Instagram!

Logistics Section Chief

ROLE

Organize and direct the service and support activities needed to ensure material needs for the site's response to a cyber incident are available when needed.

- ❑ **Identify any potential disruptions to critical infrastructure and priority services**
- ❑ **Regularly evaluate electrical system performance**
  - Consider network-reliant systems (e.g., tube system, temperature controls, etc.)
  - Deploy additional staff to manually monitor systems reliant on the network (HVAC, humidity, etc.)
  - If the fire suppression system is reliant on the technical network, activate a fire watch
- ❑ **Partner with IT/IS to identify communication redundancies for**
  - Translation services (services offered previously via telehealth may need to be brought on site)
  - Visitors, family members, clergy, or vendors (e.g., phone or video calls, end of life care)
- ❑ **Ensure food and hydration is available; consider patients, staff, visitors, and Command Center personnel**
- ❑ **Prepare for radio deployment**
  - Ensure radios are charged and there is a plan for additional batteries as needed
  - Provide just-in-time training on radio use
  - Oversee sign-out sheet to track all deployed radios
- ❑ **Ensure adequate downtime supplies: paper, toner, pencils, pens, stationary, forms, etc.**
- ❑ **Order additional supplies as needed**
- ❑ **Assess impacts to materials management and ordering processes**
  - Implement manual inventory and ordering processes for supply chain management
  - Implement a manual process for distribution, supply chain, and redistribution of clinical and operational supplies
  - Ensure availability of durable medical equipment
  - Ensure availability of oxygen
  - Ensure availability of pharmaceuticals
- ❑ **Deploy Environment of Care teams to evaluate contingency needs**
  - Clinical Engineering/Health Technology Management
  - Environmental Services
  - Facilities/Maintenance/Engineering
  - Industrial Hygiene
  - Infection Prevention
  - Physical Security
- ❑ **Assess ability to source additional technical equipment for end users (laptops, tablets, etc.)**
- ❑ **Redeploy excess staff to support operations**
- ❑ **Establish labor pool or coordinated process to redeploy staff**

  Note: Credentials and competency must be accounted for
  - Provide instructions for manual timekeeping
  - Identify staff resiliency resources (EAP, mental health, etc.) for extended incident support

To learn more about how you and your organization can prepare for a cyber event, check out the Operational Continuity-Cyber Incident (OCCI) Checklist. Be sure to check out the other available resources HHS has to offer at the Healthcare and Public Health Cybersecurity Gateway at hhscyber.hhs.gov as well as 405(d) specific resources at 405d.hhs.gov and our 405(d) social media pages: @ask405d on Facebook, X, LinkedIn, and Instagram!

Information Technologies (IT) / Information Systems (IS) Section Chief

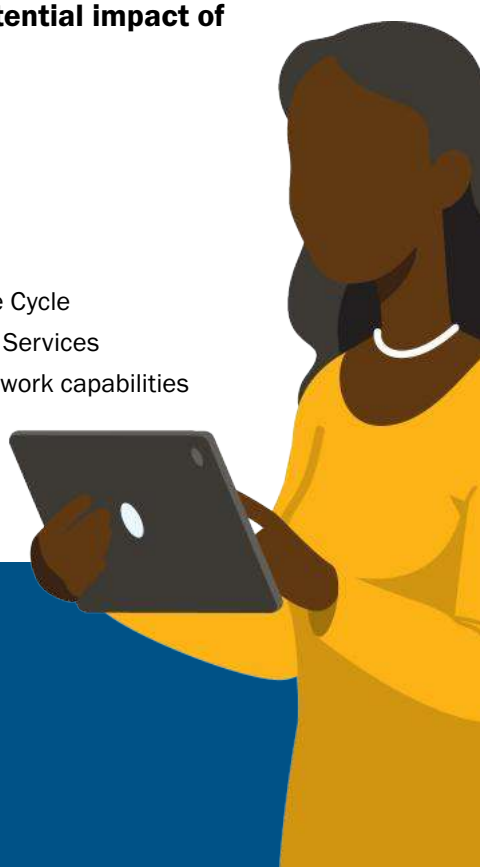
ROLE

Provide technical response, continuity, and recovery recommendations; partner with cybersecurity to inform a cyber incident response decisions and activities. Coordinates intelligence and investigation efforts.

Note: This role should be filled with IT/IS professionals.

If using an Internal Unified Command Structure, consider removing the Cybersecurity section from the Med-Tech role and place within this role.

- ❑ **Address potential IT/IS/Cybersecurity staffing needs and establish staff rotation schedule**
- ❑ **Address any qualifications or security clearance necessary based on incident complexity**
- ❑ **Triage the impact of the incident to identify segmented or usable services or applications**
- ❑ **Establish a cadence with cybersecurity for regular situation updates to inform Command**
  - Communicate scope and severity of disruption
  - Identify and communicate upstream and downstream impacts
  - Support identification and implementation of safe, alternate processes
  - Assist with restoration of technology systems
- ❑ **Identify opportunities that limit the spread of the incident. If possible**
  - Segment or isolate servers
  - Provide guidance on how to disconnect the data center from your environment
  - Quarantine or sever the connection with data centers to limit spread
- ❑ **Coordinate with internal and/or external Clinical Engineering/Health Technology Management to understand**
  - Impacts
  - Data storage limits to inform downtime processes
- ❑ **Collaborate with Cybersecurity to understand scope of disruption and potential impact of cyber incident**
- ❑ **Consider activating unified command with a cyber command structure**
  - Activate cyber insurance policy and procedures
  - Coordinate legal and risk management activities
- ❑ **Identify the impact on the following systems**
  - Bedside care: monitoring, telemetry, pumps, nurse call
  - Building systems (e.g., tube system, temperature tracking, badge access)
  - Electronic health record
  - Emergency Department/ Trauma Services
  - Imaging
  - Internet
  - Intranet
  - IS Infrastructure
  - Lab
  - Network
  - Revenue Cycle
  - Surgical Services
  - Remote work capabilities
  - Telecom



To learn more about how you and your organization can prepare for a cyber event, check out the Operational Continuity-Cyber Incident (OCCI) Checklist. Be sure to check out the other available resources HHS has to offer at the Healthcare and Public Health Cybersecurity Gateway at hhscyber.hhs.gov as well as 405(d) specific resources at 405d.hhs.gov and our 405(d) social media pages: @ask405d on Facebook, X, LinkedIn, and Instagram!

- ❑ **Establish Labor Pool or coordinated process to redeploy staff**

  Note: Credentials and competency must be accounted for
  - Provide instructions for manual timekeeping
- ❑ **At direction of CISO or Cybersecurity leader, consider proactive technical system(s) lockdown**
  - Consider data center shutdown to prohibit spread
  - Consider critical systems shutdown to limit unauthorized access to data and records
  - Consider critical systems shutdown to reduce data breach risk
  - Consider shutdown of vendor bi-directional VPN access
  - Consider shutdown of WAN connections
  - Consider lockdown of internal network segments
  - Consider fail over to Disaster Recovery, quarantine routers/switches
  - Scan all backups for integrity
- ❑ **Consider a recommendation to power down all technology to limit the spread**
  - Engage IT/IS to support network take down/recovery
  - Engage IT/IS in use of off-network computers for downtime process support
- ❑ **Establish a process for interim solution, intake, and prioritization**
- ❑ **Identify Recovery Time Objective (RTO) / Recovery Point Objective (RPO) for essential services and applications and if possible, leverage fail over options or implement disaster recovery as soon as possible.**
- ❑ **Provide updates to Command staff on estimated length of time until systems can be fully recovered (RTO/RPO in hours/days/weeks)**
- ❑ **Coordinate with Cybersecurity on timeline for threat eradication**

  Note: Re-enabling internet/WAN/VPNs may not be possible until threat is eradicated
- ❑ **Collaborate with Operations Section Chief to start a recovery plan for essential services and applications**
- ❑ **Collaborate with Incident Command on restoration and recovery processes**

  Note: This guide is for the first 12 hours; however, recovery should begin immediately
  - Identify scope of encryption
  - Reaffirm recovery time objectives
  - Validate critical application recovery priority
  - Assess critical application dependencies for recovery
  - Recover critical applications for essential business operations in a timely manner
  - Recover infrastructure

To learn more about how you and your organization can prepare for a cyber event, check out the Operational Continuity-Cyber Incident (OCCI) Checklist. Be sure to check out the other available resources HHS has to offer at the Healthcare and Public Health Cybersecurity Gateway at hhscyber.hhs.gov as well as 405(d) specific resources at 405d.hhs.gov and our 405(d) social media pages: @ask405d on Facebook, X, LinkedIn, and Instagram!