February 2021

# HEALTHCARE SYSTEM CYBERSECURITY

## Readiness & Response Considerations

ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

TRACIE
HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

# INTRODUCTION

As part of our nation's critical infrastructure, healthcare facilities large and small must be proactive and move quickly to protect themselves from cyberattacks that could directly impact the health and safety of patients and the community at large. According to medical health experts experienced in cybersecurity preparedness, cyberattacks are identified as the top threat in many healthcare systems' annual Hazard Vulnerability Analyses (HVA). The federal government, with other public and private sector partners, has worked diligently to defend against the growing number of cyberattacks on the healthcare industry.

**RELATED RESOURCES**

Cybersecurity Topic Collection

Cybersecurity and Cyber Hygiene (Issue 2 of *The Exchange*)

Cybersecurity and Healthcare Facilities (Webinar)

Lessons Learned from the Medstar Health System Outage

The U.S. Department of Health and Human Services (HHS) Office of the Assistant Secretary for Preparedness and Response (ASPR) has sponsored the ASPR Technical Resources, Assistance Center, and Information Exchange (TRACIE) since 2015. The goal of ASPR TRACIE is to fill gaps in healthcare system preparedness capabilities by providing timely, innovative ways to share information and promising practices during planning efforts. ASPR TRACIE designed this resource to help healthcare facilities, and the systems they may be a part of, understand the roles and responsibilities of stakeholders before, during, and after a cyber incident.[1] Information within this document is specifically related to the effects of a cyber incident on the healthcare operational environment, specifically the ability to effectively care for patients and maintain business practices and readiness during such an event. While the focus of this document is on disruptions associated with a large-scale cyberattack, many strategies and principles outlined are relevant to a range of cybersecurity incidents and healthcare facilities.

This document cites general cybersecurity practices; additional resources that cover more complex cybersecurity practices (e.g., those associated with medical devices) can be found in the resources section and Appendix.

ASPR TRACIE created the following ***checklists*** for operational use:

Hospital Downtime Operations Checklist

Hospital Downtime Preparedness Checklist

Cyber Incident Response Checklist

Cyber Incident System Restoration Checklist

*[1]For purposes of this resource, a cyber incident is defined as "Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein" (NIST).*

# QUICK LINKS

# PREPAREDNESS AND MITIGATION

Healthcare facility cyber preparedness incorporates industry standard security practices alongside routine exercises to assess readiness in an operational setting. In addition, regularly conducted and rigorous system evaluations serve to further identify any vulnerabilities in preparation for a possible cyber event.

## IT Incident Planning

General mitigation efforts include understanding the threats and tactics used to target vulnerabilities within a healthcare system. To keep abreast of imminent threats, cybersecurity teams and relevant medical staff should monitor official announcements for timely information on threats relevant to healthcare sector information systems. Resources such as the HHS Health Sector Cybersecurity Coordination Center (HC3) bulletins and the Health Information Sharing and Analysis Center's news updates (H-ISAC) provide crucial situational awareness information needed to effectively secure critical assets and functions. To ensure readiness, healthcare facility Information Technology (IT) teams should incorporate basic IT preparedness principles into planning protocol, including:

- Understand historical healthcare-related attacks and the subsequent lessons learned.
- Have an incident response plan and practice and update it regularly.
- Implement cybersecurity digital infrastructure checklists into operational protocols.
- Ensure enterprise and individual facilities, emergency managers, and IT teams plan collaboratively.
- Implement cyber-hygiene programs and employee education drills to prevent successful attacks.
- Identify clinical and non-clinical operational vulnerabilities within facilities.
- Identify and understand how to engage with critical external partners such as Healthcare Coalition (HCC) stakeholders.

## Cybersecurity Readiness

Effective mitigation of cyberattacks relies on careful planning by the facility or health system's IT team in conjunction with facility leadership, providers, and ancillary departments. Comprehensive routine evaluations of the facility or health system across departments and systems can provide insight into their interdependencies and expose vulnerabilities to address.

A health system's first line of defense is the information system (IS) architecture that protects the infrastructure and aims to reduce impact on core capabilities and functionality when an attack occurs.

- Within larger health systems, an ***enterprise-wide solution*** has likely been established by a team of skilled clinical and non-clinical IT IS professionals. These solutions aim to insulate the system from attack and limit its spread across multiple systems or applications.

- Medium and larger healthcare facilities should have proper ***security configuration management*** *protocols* in place. The Health Sector Council Cybersecurity resource Cybersecurity Practices for Medium and Large Health Care Organizations provides information specific to these entities.
- Separate, possibly smaller, associated facilities should ensure their ***IT cybersecurity processes are in line with the enterprise system*** and follow the same security protocols and requirements. These facilities should also ensure they have the ability to disconnect from central or enterprise systems, and run independently, to both protect themselves and the main network should an incident occur. The Health Sector Council cybersecurity resource for Small Healthcare Organizations provides information specific to supporting smaller facilities.
- Federal cybersecurity services are available at no cost to all entities. Smaller facilities, rural health centers, or others with limited IT resources in particular may explore ***free cyber hygiene services*** provided by the Cybersecurity and Infrastructure Security Agency (CISA) to identify any system vulnerabilities, evaluate resilience, and stay current on cyber practices.

## Routine Mitigation

Facilities should regularly practice vulnerability scanning to ensure patch management and other practices are effective at addressing weaknesses within the system. Investment in data backup and redundancy across the IT environment, including external mirroring, is essential for protecting vulnerable systems.

### Systems and Infrastructure Protection

- Ensure ***patch management*** policies are properly vetted and consistently executed. Keep digital technology updated with the most recent patches as they are released; prioritize patches and updates for known vulnerabilities (e.g., legacy systems). Ensure any exceptions to a formal patch management policy are approved in writing. Implementing a test environment can ensure patching and updates are done safely and with minimal impact on healthcare operations.
- Improve organizational security posture by remediating issues discovered during periodic ***penetration tests, vulnerability scans, and assessments*** used to better understand risk and the integrity of the infrastructure. Ensure scans and penetration tests include operational and physical security technology.
- Follow the National Institute of Standard and Technology (NIST) cybersecurity framework for ***system segmentation/partitioning*** where networks, functionality, and IT components are separated to control access. Streamline data flow from interconnected systems to reduce system dependencies, promote faster recovery times, and reduce the number of affected systems.
- Improve early warning of potential incidents by implementing robust ***monitoring protocols***. Map healthcare IT business practices to data flow to inform monitoring requirements. Consider establishing secondary monitoring capabilities as backup to the primary. Explore having a third-party IT consultant to assist with 24/7 monitoring and incident reporting.

- Modernize legacy systems and move towards ***virtualized data centers*** and cloud-based services. Give special consideration to securing cloud-based systems and understanding the unique risks associated with virtualized environments.
- Segregate life safety equipment and security communication platforms onto isolated networks and ***establish redundancies*** in alerting, alarms, and notifications.
- Consider establishing a Zero trust (ZT) network architecture that "moves defenses from static, network-based perimeters to focus on users, assets, and resources" (NIST 2020).
- Consider implementing use of "***Golden Images***," or offline endpoints that remain clean and are configured for a specific environment, in cases where normal workstations are affected.

## Incident Management Planning

- Review, test, and update ***IT Disaster Recovery Plans*** (IT DRP) on a regular basis. These plans should outline backup and redundancy protocols. Include emergency managers, IT teams, relevant medical staff, and stakeholders to ensure each familiarity across departments.
- Have a robust ***Incident Response Plan*** (IRP). Establish incident response processes and policies to adequately react to a cyber event including activation of the ***Incident Command System*** (ICS) whenever a service disruption occurs. Invite law enforcement, Federal Bureau of Investigation (FBI), and state/local partners to participate in IRP development.
- Ensure ***Business Continuity Plans***, Business Impact Analysis (BIA) reports, and Continuity of Operations Plans (COOP) include strategies for small and large-scale cyber incidents (i.e., short-term versus long-term, single system versus multiple).
- Plan for temporary and/or permanent ***data loss scenarios***.
- Confirm the ***Incident Management Team*** (IMT) or ICS structure addresses all aspects of the health system, including ancillary services, and that personnel are familiar with functioning within the IMT.
- Ensure emergency response planning ***includes representation from ancillary services*** and off campus locations, such as ambulatory, nutrition services, laboratory, radiology, accounts payable/receivable, communications, and legal, to avoid exclusively in-patient focused response efforts.
- Maintain an accurate and robust ***mission critical inventory list*** of hardware, software; biomedical devices; and data to inform an effective DRP. Factor in how durable medical equipment may be impacted and affect patient care.
- Consider items outside of the ***Configuration Management Database***. IT teams should collaborate with clinical engineers to acquire a list of IP/MAC/Software integral for medical equipment function.
- As new IT applications are added, ensure they are included in an IT Downtime (DT) inventory list and include a downtime plan. ***Delete obsolete IT applications*** from the IT DT inventory.

- Consider and plan for the possibility of ***control system manipulations*** compromising critical medical equipment (e.g., IV pumps or oxygen mixing/pressurization systems). Identify personnel who will oversee and assess the usability of medical equipment if an incident occurs.
- Identify ***mission critical lifesaving and life support devices*** that may be vulnerable in a cyberattack (e.g., ventilators, drug infusion pumps). When developing plans, ensure adequate backups are available or know where to procure them.
- Plan for ***regional outages impacting other healthcare facilities*** which may preclude necessary transfer of critical patients to nearby facilities.
- Communicate any emergency response changes to departments and relevant staff promptly.

## Incident Alerting

- Ensure incident response plans include instructions on how to alert and communicate in the event of degraded communications during a cyber event. Create ***internal notification protocols*** for announcing a cyber incident (e.g., paging, overhead announcement, a calling tree).
- Consider use of an ***independent mass notification system*** to ensure immediate communication with key stakeholders and staff immediately in the event of a cyber incident and during downtime.
- Consider facility or system-wide use of a phone application that would allow employees to receive ***automated alerts*** during an emergency.
- Decide on a ***need-to-know group*** for each department. Ensure alerting protocol includes staff on different shifts and schedules (e.g., on call, on leave).
- Consider developing a color code that easily communicates cybersecurity status levels. Ensure staff understand color definitions, terms, and related actions/implications.

| Example Cybersecurity Status Levels | |
|---|---|
| **Green** | Cyber security incidents and reports are at a normal level and our tools/ protections are functioning properly |
| **Yellow** | Cyber security incidents and reports are slightly higher and/or our tools/ protections are not functioning properly |
| **Red** | Cyber security incidents and reports are higher than normal and/or multiple tools/ protections are not functioning properly |
| **Compromised User** | A user fell victim to a phishing attack and gave out their username/password |
| **Compromised Device** | A device was infected by a virus/malware/etc. |

## Communication and Collaboration

- Identify a ***collaboration capability*** in cases where Hospital Command Center response coordination cannot be accomplished on-site or in-person (e.g., COVID-19 pandemic protocol).
- Explore options for use of ***virtually accessible collaboration platforms*** and applications for response needs. Policies should identify what information can and cannot be shared via this platform.
- Identify and ***setup a knowledge center capability*** (or other incident management system or response document library) to serve as an information repository. Ensure staff are trained on how to use the system (e.g., accessing specific functions, uploading/downloading documents). Consider conducting a demonstration to review where vital information will be held, what functions are available, and limitations or restrictions.
- ***Test connectivity to collaboration platforms*** and document libraries from alternate locations prior to an incident to troubleshoot issues. Proactively resolve connectivity and access issues. Ensure instructions for use and access are available offline and in print.
- Have a contingency plan ***for loss of email and voice communications*** systems such as VoIP lines (two alternatives would ensure redundancy).
- Consider using a mechanism to confirm that intended recipients have received critical communications (e.g., requiring a response back or ***read receipt***).
- Explore use of an ***out-of-band communication mechanism*** that can be used securely in the event of internal communication compromise.
- ***Have external communications templates*** prepared in advance that have been reviewed by external counsel and other necessary authorities.

## Insurance and Legal Considerations

- Ensure ***cyber insurance coverage*** is adequate for needs of the organization or facility.
- Understand when additional coverage may be necessary. While insurance may protect against general technology-related risk, ***expanded coverage may be necessary*** depending on hospital and outpatient operational requirements and risk levels.
- Know how often coverage should be reevaluated and what technology changes may prompt them.
- In case of an incident, ***cyber insurance may provide additional response and recovery resources***. Understand what services are available and how to access them.
- Ensure cyber insurance includes costs associated with a multi-week outage; use of forensics firms; ransom demands; civil and regulatory penalties and fines; and credit monitoring.
- Ensure the ***IMT are familiar with the organization's cyber insurance policies*** and other pertinent incident response reimbursement requirements.

- ***Communicate changes*** to insurance policies to relevant staff and IMT promptly.
- Consider ***legal involvement***, as it relates to issues of data protection and reporting requirements, during a cyber incident.
- Establish proper legal contracts and agreements (e.g., ***Business Associate Agreements***) with necessary vendors and third-party contractors who may assist with incident response activities.
- Consider how ***litigation or investigative activities*** may impact healthcare operations, regulatory requirements, or potential for penalties.
- Ensure all necessary ***cyber-related policies*** are in place and compliant with legal requirements and cyber coverage parameters. Consider organizational ***policies for paying ransomware attackers***. Identify who will be involved in this type of decision making. Consider using Federal Communications Commission (FCC) statutes and guidelines.

## Vendors and Third-party Engagement

- Understand how ***vendor expertise and engagement*** impact the design, performance, and protection of critical system elements before, during, and after a cyber incident.
- ***Meet with vendors pre-incident*** to discuss how impacts to systems or assets may manifest (e.g., inbound calls are interrupted but not outbound, threats to reliable life safety systems' functionality).
- In cases where equipment is not owned or managed by the facility's IT team, ***coordinate with clinical engineers and medical equipment stakeholders/vendors*** to address incident response plans, and understand associated actions.
- Plan for how a cyber incident affecting a ***third-party provider*** may impact medical operations; understand how such incidents would be communicated.

## Emergency Contact Information

- Establish and maintain robust ***emergency contact lists*** for all internal staff, ancillary units, and external stakeholders that were included in planning activities (e.g., law enforcement, vendors)
- Include ***secondary contact information*** including home addresses for critical personnel, administrators, physicians, and department heads in cases where communication is severely limited.
- Ensure contact lists include off-hours information and secondary points of contact in case primary representatives are unavailable.
- Document ***offline contact methods*** for biomedical equipment vendors. This may be an assigned account manager or cybersecurity specialist.
- Ensure designated incident response leaders have access to offline and ***hard copies of all emergency management and recovery plans*** with updated contact information for all response personnel, surrounding facilities, and relevant vendors.

## Facility Security Preparedness

- Prepare to ***manage access points*** if CCTV cameras, motion detection, alarms, and badging are impacted during a cyber event. Make ***copies of keys*** and identify staff responsible for holding, distributing, and collecting them for the duration of response efforts.
- Identify how to ***recruit additional security personnel*** or involve law enforcement.
- Plan ***workarounds for monitoring*** mother and child in labor, delivery, and nursery departments; patients and staff in psychiatric facilities; and managing visitors.
- Plan for ***securing drug cabinets*** and other locked equipment and supply closets.
- ***Develop sign-in sheets***, ensure they are included in Go Bag/Boxes. Create specific instructions for who should oversee the sign-in sheets per shift and document any additional processes that are required in conjunction with the sheets (e.g., providing IDs, signing-out, providing visitor badges). Provide instructions for where to store the sheets or who to send them to at the end of a shift.

## IT Readiness Promising Practices

- Ensure newly implemented software applications, specific to the facility, are properly vetted, integrated, and monitored by technical experts into the enterprise infrastructure.
- Ensure staff have a good understanding of their roles and responsibilities within an IMT. Review COOPs in relation to technical disruptions.
- Work closely with pertinent partners to ensure planned integrated platform linkages and/or upgrades are communicated and appropriately tested.
- Discourage "private" or "custom" developed IT applications created for individual use. If their use is vital to operations, IT and cybersecurity personnel should be made aware of their presence, proper security protocol should be implemented, and downtime procedures created.
- Consider joining trusted community threat information groups such as Information Sharing and Analysis Organizations (ISAO) or H-ISAC to maintain cyber-related activity and resource awareness.
- Consider performing a pre-purchase cybersecurity risk analysis for inbound medical equipment. Record and monitor vulnerabilities in the device's essential software.
- Have best practice policies in place to monitor legacy equipment "End of Support Dates" for contracts, purchasing agreements, and support services.
- Ensure an up-to-date user list is available offline and backed-up regularly to allow for quick identification of malicious accounts and rapid recovery. Establish a process for maintaining an active directory for new hires, transfers, and former employees.
- Consider use of downtime computers that contain copies of key medical record data from electronic health records (EHR).
- Ensure cyber hygiene strategies are consistent across all departments and facilities. Utilize several communication mechanisms to instill healthy cybersecurity practices across an organization. Consider visual aids, external email tagging, security e-newsletters, and secret surfing tests.
- Implement and understand how to enforce organizational policies for employee accountability related to cybersecurity practices. Utilize the communication plan to keep staff informed of any increased cyberattack risks.

## IT Evaluations and Assessments

System assessments serve as the cornerstone of healthcare information systems preparedness.

- Conducting a ***Business Impact Analysis*** (BIA) helps an organization determine the criticality of different hospital operations components within a health system. As part of a robust cybersecurity plan, the BIA serves to identify mission critical functions for prioritization during recovery efforts.
- In conjunction with a BIA, resumption of services during a cyber incident will also be contingent on systemic pre-identified ***Recovery Time Objectives (RTO) and Restoration Point Objectives (RPO)***. Identify and

test the RTO (downtime tolerance) and RPO (loss tolerance) to factor them into incident response and recovery plans.

- An ***Application Dependency Map (ADM)*** will also help gain insight into a hospital's IT ecosystem. It charts integral system applications and their dependencies. Like the BIA, it ensures that in the event of a cyber incident all department technologies are represented and prioritized for restoration. During a cyber incident, a proactively completed ADM can outline where to assign resources and prioritize system restoration based on impact to hospital function.
- If not using an ADM, have another standardized process in place for ***scoring criticality of all facility technologies*** that could be affected during a cyber incident. Include a strategy for integrating new software into the assessment as soon as it is operationalized. Determine how often assessments will be updated and determine a process to periodically identify new technologies.
- Establish periodic ***data custodian meetings between IT teams and leadership*** to familiarize users with IT security protocol. Socialize IT software evaluation processes with department heads to underscore the importance of completing technology assessments and mapping applications and dependencies.
- To assess an application and the related business process impacts of its disruption on operations for purposes of determining application restoration order, consider ***ranking several operational elements***.[2] If a system is affected by a cyber incident, determine its potential impact on any of the following items:
  - Patient safety/quality of care
  - Number of staff affected
  - Number of patients affected
  - Number of dependent systems affected
  - Life expectancy
  - Revenue lost (per day)
  - Legal costs/implications
  - Number of patients lost (diverted to other facilities due to impact on services)
  - Cost to enterprise, branding, image
  - Number of transactions affected

---

*[2]The Application Business Value Rating (ABVR) process, developed by Nebraska Medicine, is a business priority ranking model for applications that can be used for recovery prioritization of systems during a cyber incident.*

# Cybersecurity Exercises

Internally, organizations should regularly conduct exercises to ensure stakeholders, vendors, and emergency management personnel are prepared for a cyber emergency. Engagement in these scenarios by medical staff and ancillary components is integral to understanding downtime procedures in clinical and non-clinical settings. While frequency and intensity of exercises are not uniform for all healthcare facilities, the goal of the exercises are to find gaps in current cybersecurity practices and identify areas for improvement. To optimize exercise results, planning should include establishing timelines for remediation of results to improve upon current protocol. The Homeland Security Exercise and Evaluation Program (HSEEP) provides guidance for developing, executing, and evaluating exercises that address preparedness. CISA also maintains a library of pre-packaged exercises.

## Exercise Scenarios

- ***Develop exercises with varying degrees of impact levels*** that mimic real-world cyber incidents and address individual unit/office responses. Many exercises are restricted to specific systems, applications, or emergency situations, however post-attack summaries often reveal that limited exercises often do not align with implications of a real cyberattack.
- ***Run exercises for an array of scenarios.*** Focus on impacts to mission critical applications and subsequent effects on healthcare operations. Practice with 1-2 compromised systems and move towards larger-scale cyber incidents that impact the entire organization (worse-case-scenarios).
- ***Consider utilizing a White Hat*** (hired cybersecurity expert) to attack and stress test systems.
- ***Explore use of third-party IT specialists, or a Purple Team***, to facilitate exercises aimed at identifying vulnerabilities and providing solutions as part of an independent assessment.
- ***Conduct specific drills for paper charting and manual clinical processes***, especially for novice, new, and younger staff who may not be familiar with older manual processes. To alleviate the steep learning curve, practice hands-on and in-real-time activities versus solely providing handouts.
- ***Incorporate communication challenges into scenarios***. Run drills for internal communication issues (e.g., no phones, email, paging systems); practice answering staff and public-facing questions (e.g., news media, patients, social media).

## Exercise Frequency

- At the hospital level, routine exercises should occur ***1-2 times per year*** with individual units testing their specific workflow at least twice a year.
- At the department level, ***continuously reinforce cyber hygiene*** practices during team meetings, educational series, and other appropriate forums.
- ***Once per year***, larger organizations should run full tabletop exercises for the entire health system.

## Exercise Engagement

- ***Consider establishing a subcommittee or specialized group*** within the hospital to focus on IT security and downtime response needs to represent disparate interests within the health system.
- ***Invite IT, biomedical, vendors, and law enforcement to participate*** in exercise programs. Provide summaries and lessons learned for situational awareness when appropriate.
- ***Ensure non-medical departments and staff*** such as public relations and communications representatives are included in drills.
- ***Identify staff that may be affected with limited access to key technologies*** such as computers, Internet, specific applications. Include them in drills to determine equipment and supply needs; identify and resolve workflow issues.

## Exercise Promising Practices

- Hospital leadership and managers should ***regularly review outcomes*** during team huddles. Share lessons learned and best practices from the exercises with hospital staff.
- Ensure the protocol to activate Incident Command and downtime ***procedures are well socialized*** among staff during annual department emergency preparedness reviews.
- ***Familiarize staff with technical terminology*** and vice versa; ensure technical staff/IT teams are familiar with medical terminology pertaining to equipment and work processes.
- Use planned downtimes that occur during routine application and system upgrades to ***implement ongoing training opportunities*** for staff.
- ***Develop just-in-time training tools*** based on exercise outcomes. Use lessons learned to identify topics that may require more practice.

# Downtime Principles

In conjunction with implementing routine system mitigation efforts and periodic exercises and drills, it is critical for IT cybersecurity efforts to include ample downtime preparedness activities. Their outcomes will identify any gaps in readiness and key weaknesses in response and recovery efforts. Careful planning for downtime will save time while in the midst of a cyber event where resources are maxed.

- ***Know your plan.*** Understand requirements of the IMT structure. Determine who will fill each role. IMT expertise is critical to successful management of prolonged response and wide-scale cyber incidents.
- ***Know your workflows.*** Plan to follow the lifecycle of paper documents, have explicit instructions for which forms to use, when to use them, and where they go (paper trail). Ensure compliance with downtime procedures by establishing policies for what is optional versus mandatory. Take into consideration non-clinical services such as finance, payroll, and procurement.
- ***Know your staff.*** Pre-identify essential roles necessary for sufficient continuity of operations (clinical and non-clinical). Pre-define critical responsibilities necessary to facilitate operations and patient care within each unit. Plan for re-establishing essential roles among staff as they are moved to different departments to support altered clinical operations.
- ***Know your inventory.*** Confirm proper downtime supplies (e.g., directories; labels and forms; wireless equipment; just in time "Hot Spots," thumb drives) are readily available. Know where they are and what condition they are in; consider manual clinical equipment, administrative supplies, and ancillary needs. Identify where additional supplies can be procured and amount needed. Consider the process for ordering hospital supplies if communication is down or invoices are not accessible.
- ***Know your unit.*** Document downtime guidance for each system and critical technology that could be affected. Place documentation in centrally visible locations (e.g., red binders). Consider patient tracking; ordering supplies, pharmaceuticals, labs; results and status reporting; nourishment; and discharge needs. Create quick-start reference cards for each system. Post reference copies in highly visible areas.

## Defining and Declaring Downtime

- ***Define downtime*** for the organization and what this will activate internally. Establish a threshold for determining short-term versus long-term response. For large organizations, short-term may be three days or fewer and long-term is more than three days. Determine the amount of time that will trigger extended downtime processes be activated.
- ***Establish clear triggers***/thresholds for system shutdown; understand the complexities associated with this action (e.g., system dependencies, redundant paths).
- ***Appoint a "trigger person"*** to officially declare downtime and communicate which downtime protocol to follow (e.g., short-term, long-term). This is normally the lead Incident Commander.

- Identify health system policies for ***who is authorized to shut down a system*** and carry out related actions (e.g., disconnect the organization from the internet, divert ambulances, and/or shut down email, external VPN connections, pay/not pay ransom, notify law enforcement/FBI, state authorities). In extreme cases, immediate shutdowns without leadership approval may be necessary.
- Authorize a clear ***escalation plan*** for alerting staff, leadership, and stakeholders. Include notification protocol for alerting local law enforcement or other federal officials (e.g., intelligence fusion centers, FBI, U.S. Secret Service, U.S. Department of Homeland Security).
- Align downtimes with business impact analysis and disaster recovery plans. Consider ***categorizing downtimes*** based on their impact to operations (e.g., Category A is 12 hours or less time down, Category B is more than one day down, Category C is more than three days down). Classifying downtime ensures corresponding response activities meet the severity of the cyber incident but are pursuant to the organization's level of risk tolerance.

## Downtime Workforce Preparedness

Workforce leadership, in conjunction with department heads, should plan for disruptions to normal work schedules and activities during downtime. Resources may be reallocated to support highly impacted units/departments. Some staff may be required to take time off or work from home if services are decreased or the IT capabilities required to do their jobs are unavailable.

- ***Communicate to workforce*** that in the event of a severe cyber event they may be required to work longer than normal hours, or in some cases less than normal hours.
- Proactively identify:
  - Who is essential?
  - What services are critical?
  - What is the minimal staffing needed?
  - What institutional policies support mandatory use of paid time off (PTO), remote work?
  - What services would be cut in different scenarios?
  - What is the policy for reducing workforce due to decreased services?
- ***Plan for the possibility of a 24/7 schedule*** to be implemented for some staff (IT, security, administrative, managerial, and select ICS roles).
- Consider whether there are adequate ***cross-trained resources to supplement staff***; if not, identify where additional resources can be procured (e.g., volunteers, state, local, territorial, and tribal [SLTT] resources, staff from unaffected facilities).
- Determine who will be required to ***assist with long-term recovery efforts*** (e.g., re-entering data, reconciling documentation, testing/validating medical equipment).

- Determine who might be assigned to ***work from home*** and their equipment and supply needs.
- Identify ***potential resource gaps*** in clinical versus non-clinical settings that may occur as a result of system(s) or application(s) that are brought down. Prepare beforehand to alleviate real-time resource gap analysis and ensure rapid mobilization of people and resources.
- Think through ***compensation policies***, provision of proper ***workforce support*** (daycare services, spousal support, transportation services, lodging); consider impacts on exempt and non-exempt staff. Ensure policies consider any relevant labor/union, employment laws, SLTT regulations, human resources policies.
- Establish alternate processes for conducting hiring, orientation, and personnel evaluations during an extended downtime response.
- Identify standard work processes or tasks that will need to be adjusted to support staff.

## Downtime Documentation Promising Practices

- ***Identify a process to transfer medical record/essential medical documents*** to other facilities and providers during a cyber incident if needed.
- ***Maintain downtime plans in multiple formats*** (e.g., on the intranet, thumb drives, in print) for rapid distribution during a response.
- ***Develop standardized downtime forms***. Avoid creating department-specific forms unless required to meet facility needs. Include precise instructions for use; flag critical information that must be collected. Downtime forms should mimic the format of forms already in use for easier adoption.
- ***Create a Go-Bag/Box*** for each department with downtime forms, essential reference information, quick start cards, checklists, and key instructions. Include reminders for standardizing information (e.g., dates should be date of service, not date of entry). Distribute to a centralized location within each department and ensure staff know where they are located and how to use them.
- ***Ensure proper backup documentation*** is available in various formats if shared drives are down. Have instructions ready for accessing documents and resources.
- ***Ensure up-to-date critical medical guidelines*** and clinical reference materials are available offline or in multiple formats. If physical materials will be made available, have multiple copies (e.g., Physician's Desk Reference).
- ***Establish a routine*** for periodic downtime form reviews and updates, especially when new technology, applications, or workflows are introduced.

# RESPONSE

When a cyber incident is suspected, IT experts will immediately begin to assess the level of impact to each system or infrastructure. As they investigate the extent of the damage and move to isolate, repair, or remove affected technologies, the hospital IMT will activate to stabilize hospital operations and maintain safe patient care. The following steps can help ensure a smooth initial response:

- The IMT (or a similar counterpart) will ***determine the scope of an event*** to initiate and manage the correct response. Response efforts should be based on pre-determined severity/impact definitions. Levels of system downtime will correlate to the scope of impact to IT infrastructure.
- Each healthcare system and facility should ***know their thresholds for what triggers a system*** shutdown. Entrusting IT teams and delegating authority to immediately lockdown a system or systems once thresholds have been reached is crucial to mitigating further damage.
- ***Implement Business Continuity Plans***/COOP upon activation of an IMT.
- Ensure inclusion of ancillary representatives and partners in all aspects of response. Follow established protocol for integration and periodic ***communication with Healthcare Coalitions***, Healthcare System Command Centers, and other emergency management groups as appropriate.
- ***Ensure compliance*** with enterprise, Federal, or SLTT disaster response requirements.

**These checklists can help healthcare facility personnel prepare for and manage downtime due to cyber incidents:**

Hospital Downtime Preparedness Checklist

Hospital Downtime Operations Checklist

## Incident Command Principles

Once the threat and impact level have been confirmed, the IMT should follow protocols that correspond to the scope of the cyber event. Each incident will differ in degree of impact and require a combination of response and recovery strategies. General principles and promising practices are to:

- Include personnel with a ***depth of cybersecurity skills*** on the IMT. If the incident is beyond the current team's abilities, obtain additional resources based on recruiting options outlined in the IRP.
- Ensure the IMT is comprised of ***representatives from all functional areas*** of the hospital/health system, including clinical, non-clinical, support, and ancillary departments.
- ***Be inclusive across departments***. Include IT personnel in all aspects of Incident Command communications, meetings, and operational decision making. Conversely, representatives from clinical, non-clinical, and administrative departments should be integrated into IT team recovery planning efforts.

- Identify additional/supplemental staff to ***replace IMT members*** that may not be able to fulfill their duties due to other responsibilities, or illness.
- Organize an initial ***Incident Command brief***. Identify what capabilities are available, secure, and best suited to facilitate a large meeting (e.g., bridge lines, collaboration platforms). Include enterprise leadership, department chiefs/chairs, technical experts, legal counsel, and public relations personnel on the initial brief. Determine a cadence for routine updates.
- Establish operational periods to cover the response and the IMT personnel assigned to each time period. Recognize the ***IMT structure may be modified*** as response efforts change based on evolving response objectives and operational needs.

## Workforce Resilience

Depending on the scope of the event, departments and facilities may require additional or reallocation of staff during downtime. Altered workflows may increase workload and slow throughput. Proper human resource and compensation policies should be in place to readily implement or alter work schedules and other related matters. Workforce leadership should conduct a real-time inventory of available staff to plan for reallocation of resources to assist with response and recovery efforts in different departments. Other steps that can bolster workforce resilience include:

- ***Continuously communicate the scale and expected duration of downtime*** to staff so they can plan accordingly. When staff understand the severity of a cyber event, there is greater compliance with downtime procedures and recovery efforts. It also decreases stress, frustration, and anxiety.
- ***Identify where necessary support can be found*** in cases where additional cyber skill sets may be necessary (e.g., IT support from vendors, cyber insurance provider, ancillary facilities).
- ***Identify essential staff*** early that may need to work altered or extended schedules during the response effort. Plan for 24/7 work periods for critical recovery personnel. Consider addressing needs for personal support such as childcare and nutrition.
- ***Transition staff from departments with decreased staffing*** needs/services to areas in need of supplemental staff (e.g., nursing staff can be moved from a surgical unit to assist with ED activities).
- ***Ensure workforce transferred to recovery efforts have necessary skillset*** to properly assist each department. They should be familiar with the software applications and operational workflows within that department or have a training plan established.
- ***Implement proper orientation, mentoring, and/or supervision*** before re-deploying staff to assist in new areas to ensure patient safety and effective job performance. Specific tasking should be identified and briefed prior to transitioning staff.
- ***Identify senior staff to provide additional downtime training***; organize sessions for efficiency; utilize quick start cards to reinforce information. Despite exercises, during a cyber event, staff will still require just-in-time training. Consider, where possible, assigning senior personnel to mentor less experienced personnel.

- ***Consider using offsite staff*** (from non-affected facilities) to supplement staffing shortages (e.g., health information manager, finance staff, clinical support, or compliance/privacy officials).
- ***Review regulatory and certification requirements*** to ensure altered staff assignments and duties meet regulatory or licensing mandates. Consider relevant labor/union or other employment laws, regulations, and policies.

## Response Downtime Procedures

Departments should be prepared to quickly move to use of downtime forms and manual charting processes in a cyber event. The health system IMT should continuously estimate downtime timelines and adjust response procedures as needed for effective response.

## Downtime Forms

- ***Document and distribute any new or updated workarounds*** to leadership/staff immediately so protocol can be updated across the organization.
- ***Err on the side of enacting longer downtime procedures to reduce ambiguity*** in cases where it is difficult to determine downtime timelines due to the scale of a cyber event.
- ***Establish a downtime team***—familiar with the process—is in place to support staff as distributing, implementing, and utilizing downtime documents will be time consuming.
- ***Verify that downtime documents being used are current***; if new forms need to be generated, ensure they go through proper approval channels.
- ***Consider security requirements for records, files, charts, documentation***, and forms that may contain Personally Identifiable Information or require Health Insurance Portability and Accountability Act (HIPAA) compliance. Secure all hardcopy data and financial information.
- ***Ensure new downtime operational processes meet prescribed regulatory agency requirements*** for data submission, site visits, and the like.

## Operational Considerations

- Ensure processes at all affiliated facilities, campuses, and institutions are consistent where appropriate to ***avoid discrepancies in record keeping/documentation*** and to ensure quality of care.
- Ensure the knowledge center (or other ***incident management system*** or response document library) is being utilized appropriately.
- Determine how basic patient information (e.g., demographics, medical history, medications, allergies, family phone contacts) will be maintained (e.g., printed snapshot at admission) if access to EHR is limited or not possible. If your state has a ***Health Information Exchange***, establish procedures to access this information in lieu of the EHR.

- Consider how ***disrupted voicemail services will affect communicatio***n, especially for case managers, nurses, and providers with no direct lines who depend on voicemail to relay critical patient care data.
- Address possible ***impact to online patient portals***. Consider how patients will access related records and adjust requirements for patient access to their health information to ensure compliance with applicable requirements (e.g., the Information Blocking and Interoperability Regulations, HIPAA).
- Understand ***options to reduce patient volumes*** (e.g., cancelling elective procedures and appointments, diverting ambulances), when they should be implemented, and for how long based on the scale and expected duration of the event. Attempt to forecast a timeline for these actions and communicate to surrounding health facilities/partner hospitals.
- ***Plan for possible regional outages*** impacting other healthcare facilities that may preclude necessary transfer of critical patients to nearby facilities.
- ***Identify units that may need additional support for new staff*** unfamiliar with manual operations and paper charting; provide these departments with additional training support. Provide downtime example forms (e.g., how to write safe clinical orders for medication/therapy).

## Personnel Adjustments

- Consider how to ***use employees that are unable to work*** due to impact on computer systems within the confines of labor/union, employment laws, and staffing policies.
- ***Designate personnel on the floor*** to identify resource gaps (who needs help, what are the specific tasks, which require more resources) and match/deploy talent to meet the need.
- Designate available ***personnel to serve as runners*** and perform other roles when communication systems are impacted (e.g., tube stations/messaging systems are down, answer phones, scribe).
- Consider having pharmacists move to the floor to support providers. If using paper forms, ***ensure a way to confirm medicine orders*** (correct dosage, patient, route, timeline). When filling out forms, ensure writing is legible, information provided is compliant, and contains all necessary data points.

## Clinical Promising Practices

- ***Establish a process for how orders will be created, collected, and communicated to hospital runners***. For departments such as food service and cleaning that will likely remain busy, avoid having departments call-in their orders unless there is a designated person to answer the phone and coordinate requests. Create a standard process to log, reference, and close orders.
- ***Set up workstations for collecting, organizing, and storing manually written medical records***. Organize files so that it is easy to identify patients based on location within the unit/hospital.
- Ensure departments use the proper Medical Record Numbers (MRNs) (i.e., designated downtime MRNs) versus previous MRNs to avoid conflict and confusion.
- ***Create workarounds in case of limited access to business continuity data*** and information such as station reports/patient information. Having IT staff focused on accessing patient information can be resource intensive, impacting recovery.
- ***Consider postponing routine administrative tasks*** such as staff annual evaluations or new hire onboarding when HR services are disrupted. Identify critical forms and services that may be altered (e.g., credentialing, job applications, benefits information, claims data, HR incident reports). For those situations where delays are not possible, implement approved workaround plans.
- ***Document all cyber related recovery activities*** for emergency reimbursement (even if it is unclear what is allowable).
- ***Define and communicate how staff may use personal devices*** (e.g., smartphones, tablets) as contingency communication tools during response downtime, especially for staff working from home or in off-campus locations. Clarify and communicate what is prohibited.

## Communication/Information Sharing

During a cyber event, effective information sharing is vital to adequate response and recovery efforts. Proper communication directly impacts a hospital's ability to recover from a cyber-event while keeping stakeholders informed and safeguarding patient safety. Consider the following steps to ensure information is shared clearly and consistently during an incident:

- ***Initiate the communication plan to manage messaging*** and ensure consistency when providing status updates to relevant internal and external stakeholders (e.g., staff, patients, visitors, vendors, insurers, media, and HCCs).
- ***Decide what information will be disseminated***, how often, and in what manner. Appoint a representative(s) to speak on behalf of the organization. For larger health systems, there may be several Incident Command structures to communicate with across facilities.

- ***Coordinate messaging*** by establishing a communication approval process that validates information and ensures compliance with legal requirements. Be familiar with hospital, corporate, HCC, public relations, and legal department communication protocols. Ensure messaging aligns with that of stakeholders and partners to avoid mixed messaging.
- ***Manage accurate and timely messaging*** to establish trust and mitigate false narratives. Create a communication workflow to funnel information from multiple points to a single channel/IMT.
- ***Create a cadence for status updates***. Simplify technical or clinical information to avoid confusion. Ensure the pace of communication matches the intended audience (e.g., some staff may not be able to check email several times a day).
- ***Continually monitor news outlets and social media*** to stay aware of trending misinformation, public sentiment, and information gaps. Decide what messages are urgent and which are for general knowledge and transmit using the appropriate tool.
- ***Consider whether the local HCC can/should be notified*** and if they are able to share incident information and alerts with their members.
- ***Consider utilizing CISA Priority Telecommunication Services*** (PTS) that are available to critical infrastructure organizations for emergency contingency communications.

## Internal Communications

- Identify the best way to ***convey internal messaging*** using the communication plan (e.g., PA systems, postings, VOIP, analog phone, portable radios, backup mobile communication devices or apps, clinical low voltage phones).
- ***Utilize collaboration platforms***/communication tools (e.g., Microsoft Teams, WebEx) that are available and can be used to securely facilitate longer term collaboration needs.
- Consider utilizing other existing communication channels for ***ongoing outreach efforts*** (e.g., E-newsletters, Zoom forums, town halls). When communicating downtime estimates internally, use specific units of time, not ambiguous phrases.
- ***Plan the battle rhythm*** of meetings early and ensure the rhythm matches new operational workflow (i.e., do not over communicate or under communicate). Identify the best times of day to communicate with staff (e.g., not during shift changes or morning rounds) and external stakeholders.
- ***Tailor key talking points*** for leadership and section chiefs to deliver to multiple audiences.
- Ensure Incident Command leadership and department heads make time to engage with staff throughout the response. Leadership rounding to engage with staff can ensure a well-received communication effort.
- Be prepared to answer ***questions from patients and staff*** on whether they or their data were impacted, released, or taken.
- Expect that any information disseminated internally may be disseminated publicly.

## External Messaging

- Be prepared to have ***information sharing constraints*** imposed by law enforcement and/or other authorities. In some cases, information may be restricted depending on vendors, law enforcement, organizational, or federal policies. Ensure communications teams are aware of any information sharing limitations/restrictions.
- Be prepared to ***answer questions from media, elected officials, regulators and the public*** related to the incident, and anticipate requests for information (e.g., is our data safe? Is your system safe?).

**This checklist can help healthcare facility personnel respond to a cyber incident:**

Cyber Incident Response Checklist

- Determine the need to ***establish regular communication with regulatory agency(s)*** (e.g., local health department, HCCs, The Joint Commission, CMS). Assign point of contact to make expected updates.
- As a best practice in larger-scale cyber incidents, consider ***avoiding media interviews***. Using exclusively written statements (at least at the onset of an incident) controls the message and can help avoid any legal or compliance issues.
- Advise staff and leadership ***not to speculate as to the cause and effect of a cyber incident*** over email, which can be discoverable in subsequent civil actions.
- Identify and ***use external advisors*** (aside from legal) to assist with media relations; leverage public relations networks to your advantage to control messaging.

## Facility Security Considerations

With normal security services altered or potentially unavailable, changes to security protocol will need to be addressed.

- ***Know where all controlled access points are***, provide keys to necessary staff, and recruit additional security personnel to monitor locked units. Involve hospital security and/or local law enforcement.
- In special security/access restricted departments, ***consider use of additional officers***/personnel (stationary vs. rounding).
  - » Plan workarounds for monitoring mother and child in labor, delivery, and nursery departments.
  - » In psychiatric facilities, enact alternate sign-in and security protocols.
  - » Station additional security staff at doors and entrance/exit areas.
  - » Determine if there is a need to restrict visitors.
  - » Develop plan for securing and providing access to drug cabinets.
- Ensure ***sign-in sheets are being utilized*** according to instructions and are logged at the end of a shift.

## Safety Considerations

- Ensure open lines of communication between IT response teams and departments to flag safety issues as soon as they arise. Create a reliable incident reporting mechanism with tracking capabilities.
- Safety officers, patient advocates, and case managers should move to the patient care areas for routine monitoring to proactively identify areas for improvement and provide safety reminders.
- Report adverse patient impact incidents to the appropriate lead; make external notifications as appropriate. Create a workflow to share, distribute, and collect safety forms to report incidents (e.g., Microsoft forms) and identify a repository to process and store these reports.
- Avoid pharmacy medical order incidents by ensuring downtime forms include required safety components (dose range, proper units, frequency, timeline, dose route). During downtime, most safety events are related to medical orders that do not include all necessary information. Note drug interaction and allergy alert software/verification may be unavailable and increase potential risk.
- Ensure new/less experienced clinical staff know what components are required for medical orders. Without an EHR to reference as a decision support tool, highlight critical information, and standardize order sets, vital information may be neglected. Consider utilizing pre-printed order sets (e.g., sepsis, diabetic ketoacidosis) for high volume/high consequence orders.
- Create forms for high-risk medications/any medicine with an associated protocol (e.g., insulin drip).
- Demographic information may not be available on downtime reports (e.g., BCA reports). Identify alternative capabilities to verify patients.

## Downtime Financial Promising Practices

- Have alternatives for providing financial counseling to patients while systems are down. Consider use of pre-printed brochures; listing helpful resources and organizations; or providing alternative points of contact for counseling.
- Consider setting up a separate cost center for tracking purposes. Decide what to do with invoices and other billing documents that cannot be immediately scanned.
- Track response costs by unique categories (e.g., personnel, equipment, supplies, lost revenue).
- Work to address patient reimbursement issues with third party payors.
- Have workarounds to collect co-payments and cash; determine how to pay staff if payroll systems are affected. Consider payment needs for food, pharmacy, gift shop, parking, and other services.
- Consider providing emergency or Incident Command leadership with a funding allotment for discretionary spending on necessary supplies (e.g., technical equipment, office supplies).
- Notify supply vendors early of any problem(s) and agree on response procedures to be followed.
- Establish communication with CMS to support billing and other services.
- Notify third party payors early of issues with billing systems to establish possible workarounds and avoid penalties.
- Dispatch financial staff to help monitor admitting, discharges, and transfers (ADT). Ensure patient registration and coverage information is correctly recorded.

# RECOVERY

Severity of the cyberattack will inform the length of recovery time. While some restoration will be immediate, long-term recovery and a return to normal operations will entail continual analysis and adjustment. Systems will NOT be restored at once. With each modification departments must monitor operational safety and security. Recovery efforts across departments could be resource intensive. If possible, confirm the attack is no longer occurring or will not continue to occur.

**This checklist can help healthcare facility ensure systems are restored after a cyber incident:**

System Restoration Checklist

- ***Consider recovery as a continued part of downtime.*** As departments and systems are restored, assess the level of functionality that would be beneficial or detrimental to operations (e.g., if a system is only partially functioning, do the missing capabilities hinder workflow, or increase risk?)
- ***Plan for migration of manual documentation back to electronic format*** once systems are restored. Think through the downstream effects on staff during this arduous process (while still needing to do their "day jobs").
- ***Available staff will need to continue to provide extra support*** to help with high volumes of data entry and charting reconciliation. IT personnel and others may need to continue to work long hours to bring-up, test, and resolve ongoing system issues as they come back online.
- A determination may be made that ***some manually recorded data will not be reconciled*** with the EHR; instructions on what this information is and how it will be stored will need to be given.
- ***Some IT applications may be determined non-recoverable*** and hence new alternatives will have to be used moving forward.
- ***Workforce leadership will need to plan for mobility of staff*** and how to meet workforce needs on a long-term basis. Consider long-term effects on workforce (e.g., childcare, mental well-being, spousal/partner support). Identify where additional support staff can be found.
- ***Consider if vendors can assist with reconstitution of biomedical records*** and support additional recovery needs for specialized biomedical equipment.
- ***Resume any suspended diagnostic or therapeutic in-patient procedures*** as soon as conditions allow. Implement a process for contacting patients whose outpatient appointments were postponed and make arrangements for rescheduling. Where appropriate plan to repatriate any transferred patients, who wish to return.
- ***IMT should collaborate with communications leads and establish a process for providing updates*** to external stakeholders. Decide on a status format, who the need-to-know group is, and how often updates will occur. Use simplified language that avoids technical or clinical jargon. Ensure messages follow information sharing restrictions.

- ***Recovery may involve reloading/patching software*** on capital medical equipment. Involve clinical engineering staff and service providers to schedule such activities.

## Financial Recovery

Financial recovery spans the entirety of the revenue cycle. Health Information Management (HIM) is an integral part of recovery efforts to ensure the integrity of the cycle from patient registration to claims processing, and collection of payments. In the event of a cyber incident, financial teams will need to identify what recovery activities will be conducted by HIM resources. The following steps can ensure the financial recovery process is as smooth as possible:

- Begin ***collecting response related financial data early*** and continue to follow an outlined submission process and format.
- ***Explore insurance options*** to assist with revenue loss and disruption.
- ***Hold all accounts*** with service dates within the incident timeframe.
- Have ***finance SMEs integrated into recovery meetings*** for insight on timelines to manage expectations and plan ahead for ongoing recovery efforts.
- HIM partnerships with compliance and providers are important for ***reconciling downtime charting/documentation***.
  - While working to ***reconcile deficiencies in records***, start coding from paper charts while waiting for systems to be restored.
  - The number or personnel to perform coding will likely need to be increased; consideration should be given to hiring a vendor to assist if needed.
  - ***Implement a record QA process***, and flag all deficiencies to be reconciled at one time
  - Do not aggressively pursue providers for deficiencies that are not a major issue to avoid overburdening; wait a reasonable amount of time for signatures.
- Develop a ***finance policy for finalizing closure of records*** when signatures cannot be verified. Use a stamp or authorized marking to identify records that have been audited, reconciled, and closed.
- Ensure dates are correctly marked for revenue integrity. For any manual charge entries that take place, ***ensure consistency in the charge entry process*** and document that workflow.
- Assimilate needed damage claims documentation for submission according to prescribed outlines set by the insurance company, FEMA, or other reimbursement provider.
- When appropriate, begin ***reimbursement and insurance claims***.

## Demobilization

- Define ***criteria for declaring the incident over*** and returning to normal operations. Notify proper stakeholders. Prepare final media statement and update websites, intranet, and phone services.
- Collect documentation for ***after action reports, lessons learned, and corrective action/improvement plans***. While the incident is still fresh, complete hot washes at shift change or other announced time periods set by the Incident Commander.
- Identify a ***repository to hold post-incident data***. Include documentation for any new downtime forms or workflows and safety or security incidents.
- Distribute a ***timeline for post-incident activities*** with deadlines to ensure compliance.
- ***Inventory Incident Command supplies*** and complete the replenishment process.

# ACKNOWLEDGMENTS

*This document was developed by ASPR TRACIE, in collaboration with our primary contributors MedStar Health and Nebraska Medicine, and ASPR TRACIE Senior Editor, **John Hick**, MD, Hennepin Healthcare.*

## MedStar Health

**Craig DeAtley**, PA-C, Director, Institute for Public Health Emergency Readiness, MedStar Washington Hospital Center

## Nebraska Medicine

**Lisa Bazis**, MS, Chief Information Security Officer; **Brian Fox**, MBA, PMP, Director, Strategic Planning & Operational Alignment; **Marc Ferguson**, MBA, MCSM, AFBCI, CBCP, Executive Director, IT Operations; **Shelly Schwedhelm**, MSN, RN, NEA-BC Executive Director, Emergency Management and Biopreparedness, Nebraska Medicine and Global Center for Health Security; and **Dawn Straub**, MSN, RN, NEA-BC, Executive Director, Nursing Professional Practice and Informatics

*The ASPR TRACIE Team would like to thank its team members and the following subject matter experts who reviewed this document in January 2021 (listed alphabetically):*

- **Eric Alberts**, CEM, CHEP, CHPP, Corporate Director, Emergency Preparedness, Orlando Health
- **American Hospital Association**
  - **Samantha Burch**, MA, Director, Health IT Policy
  - **John Riggi**, Senior Advisor for Cybersecurity and Risk
  - **Roslyne Schulman**, MBA, MHA, Director, Outpatient Payment, Emergency Preparedness and Response, and Public Health Policy
- **ASPR Critical Infrastructure Protection (CIP)**
  - **Robert Bastani**, CISSP, CISM, CRISC, Senior Cyber Security Advisor, Healthcare and Public Health Sector
  - **CDR Thomas Christl**, MS, Branch Chief, Infrastructure Analysis & Partnerships
  - **CAPT James Czarzasty**, RPh, MS, Division of Critical Infrastructure Protection
  - **Laura Wolf**, PhD, Director, Division of Critical Infrastructure Protection
- **ASPR National Healthcare Preparedness Programs (NHPP)**
  - **Scott Dafflitto**, JD, MPH, HHS ASPR NHPP
  - **Angela Krutsinger**, HHS ASPR Field Project officer Region VII
  - **William Mangieri**, HHS ASPR HPP Field Project Officer Region VI
  - **Brittney Seiler**, MPA, HHS ASPR NHPP
  - **CAPT Duane Wagner**, USPHS, HHS ASPR HPP Field Project Officer Region V
- **Lynne Bergero**, MHSA
- **Paul Biddinger**, MD, Medical Director, Emergency Preparedness, Mass General Brigham, and Medical Director, Massachusetts General Hospital

- **Caecilia (Cece) Blondiaux**, Division of Acute & Continuing Care Providers Quality, Safety & Oversight Group, Centers for Medicare and Medicaid Services (CMS)
- **Don Boyce**, JD, Vice President, Emergency Management, The Mount Sinai Health System
- **Garrett Hagood**, Director, Special Initiatives, Chief Information Security Officer, Coastal Bend Regional Advisory Council (TX)
- **Healthcare Ready**
  - **Temitope Akintimehin**, MPH, Senior Program Analyst
  - **Nicolette Louissaint**, PhD, Executive Director
  - **Courtney Romolt**, MA, Senior Program Analyst
- **Healthcare and Public Health Sector Coordinating Council Cybersecurity Working Group**
  - **Greg Garcia**, Executive Director, Cyber Security, Health Sector Coordinating Council
  - **Suzanne Schwartz**, MD, MBA, Director, Office of Strategic Partnerships and Technology Innovation, Center for Devices and Radiological Health, US Food and Drug Administration (FDA)
  - **Allison Burke**, Program Operations Lead, Health Sector Coordinating Council
  - **Michael Wargo**, RN, BSN, MBA, PHRN, Vice President, Enterprise Preparedness and Emergency Operations, HCA Healthcare
  - **Jessica Wilkerson**, Cyber Policy Advisor, All Hazards Readiness Response and Cybersecurity Team, Center for Devices and Radiological Health, FDA
- **James Paturas**, DHSc, CEM, EMTP, Director, Center for Emergency Preparedness and Disaster Response, Yale New Haven Health
- **Mary Russell**, EdD, MSN
- **Mitch Saruwatari**, Director, Emergency Management, Kaiser Foundation Hospitals and Health Plan, Inc.
- **US Department of Health and Human Services**
  - **Julie Chua**, PMP, CAP, CISSP, Risk Management Branch Chief, Office of Information Security
  - **A. Kevin Dang**, Cyber Security Program Analyst, Aveshka
  - **Nick Rodriguez**, HHS 405(d) Aligning Health Care Industry Security Approaches Program Manager, Office of Chief Information Officer
  - **Greg Singleton**, Director, Health Sector Cybersecurity Coordination Center (HC3)
- **US Department of Homeland Security, Cybersecurity & Infrastructure Security Agency (CISA)**
  - **Stephen Curren**, MS, Associate Director, Planning and Coordination, National Risk Management Center
  - **Andrea Fendt**, National Risk Management Center
  - **Jonathan Halperin**, MS, Senior Cybersecurity Liaison
  - **Jonathan Homer**, MS, ISC2, CISSP, Branch Chief, Threat Analysis, Threat Hunting
  - **Briana McClenon**, National Risk Management Center
  - **Ashley Montgomery**, External Affairs Advisor, National Risk Management Center, Office of External Affairs

## Resources Related to Cybersecurity

- **ASPR TRACIE:**
  - Critical Infrastructure Protection for the Healthcare and Public Health Sectors
  - Cybersecurity Topic Collection
  - Healthcare Preparedness and Response Capabilities
  - Exchange Critical Issues in Healthcare System Preparedness Cybersecurity
  - Paper Based Hospital Records When EHR are Inoperable
- **Association of Healthcare Emergency Preparedness Professionals: Cyber threats to the Healthcare Sector**
- **BMC Medical Informatics and Decision Cybersecurity of Hospitals**
- **California Emergency Medical Services Authority:**
  - Incident Planning Guide: Information Technology (IT) Failure
  - Incident Response Guide- Information Technology (IT) Failure
- **California Hospital Association: Business Impact Analysis Hospital Continuity Planning**
- **County of Santa Cruz Health Services Agency: Business Continuity Plan Example**
- **CREST: Cyber Security Incident Response Guide**
- **Cybersecurity and Infrastructure Security Agency (CISA):**
  - Alerts and Tips
  - Cyber Hygiene Services
  - Cybersecurity Insurance
  - Cybersecurity Quick Links
  - Ransomware Guidance and Resources
  - Security Tip (ST19-002)
  - Supply Chain Risk Management Essentials
- **Department of Health and Human Services:**
  - ASPR Critical Infrastructure Protection Bulletin Distribution List Registration
  - Critical Infrastructure Protection for the Healthcare and Public Health Sectors
  - Cybersecurity Checklist
  - Health Sector Cybersecurity Coordination Center (HC3)
  - Joint HPH Cybersecurity Working Group/405(d) Program
    - Health Industry Cybersecurity Practices

- Cybersecurity Reports and Tools- Managing Cyber Threats and Risks
- Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations
- Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations

- **Department of Homeland Security:**
  - A Lifeline-Patient Safety and Cybersecurity
  - Cyber Tabletop Exercise for the Healthcare Industry
- **Federal Bureau of Investigation**
  - Internet Crime Complaint Center ICR
  - FBI Field Offices
  - InfraGard
- **Federal Emergency Management Agency: Incident Command System Resource Center**
- **Food and Drug Administration**
  - Cybersecurity Digital Health Center of Excellence
  - Medical Device Safety
- **Health Information Sharing and Analysis Center: H-ISAC**
- **Health Information Trust Alliance: Health Plans Cyber Simulation Exercise After-Action Report**
- **Health Sector Coordinating Council:**
  - Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)
  - Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM)
- **Indiana Government: Cybersecurity Training and Exercise Guide**
- **International Medical Device Regulators Forum: Principles and Practices for Medical Device Cybersecurity**
- **Iron Mountain: When Cyberattacks Hit, Disaster Recovery**
- **National Institutes of Standards and Technology**
  - Contingency Planning Guide for Federal Information Systems
  - Identifying and Estimating Cybersecurity Risk for Enterprise
- **National Rural Health Resource Center: Cybersecurity Toolkit for Rural Hospitals and Clinics**
- **Massachusetts General Hospital Center for Disaster Medicine: Massachusetts General Hospital Center for Disaster Medicine**
- **MITRE: Medical Device Cybersecurity**

- **Ohio Healthcare Information and Management Systems Society:** Incident Response Tabletops
- **Ready.Gov:**
  - » Business Impact Analysis
  - » IT Disaster Recovery Plan
- **Sample** Cyber Incident Lessons Learned Finance Section
- **SUNY Downstate Health Sciences University:** Incident Command Center Plan