HEALTHCARE SYSTEM CYBERSECURITY

Readiness & Response Considerations

Originally Published February 2021, Updated October 2022

ASPR
Administration for Strategic 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. According to medical health experts experienced in cybersecurity preparedness, cyberattacks have been identified as the top threat in many healthcare systems' annual hazard vulnerability analyses (HVA). In response, the federal government, alongside public and private sector partners, continues to work diligently to defend against the growing number of cyberthreats on the healthcare industry.

The U.S. Department of Health and Human Services (HHS) Administration of Strategic 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]

RELATED RESOURCES

Cybersecurity Resource Page

Cybersecurity Topic Collection

Cybersecurity TA Responses

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

Cybersecurity and Healthcare Facilities (Webinar)

Healthcare System Cybersecurity: Readiness & Response Considerations (Presentation) (Webinar)

Lessons Learned from the Medstar Health System Outage

The information included in this document is specifically related to the effects of a cyber incident on the healthcare operational environment, and one that impacts 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 cyerattack, many strategies and principles outlined are relevant to a range of cybersecurity incidents and healthcare facilities.

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

[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).*

ASPR TRACIE created the following ***checklists*** for operational use before, after, or during a cyberattack:

Hospital Downtime Operations Checklist

Hospital Downtime Preparedness Checklist

Cyber Incident Response Checklist

Cyber Incident System Restoration Checklist

QUICK LINKS

This document focuses on cybersecurity planning related to the following key actions:

1. Ensure constant surveillance of the system
2. Identify triggers and go to immediate shut down and escalation of issue
3. Communicate to all stakeholders
4. Implement business continuity processes
5. Implement downtime recovery processes

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 technical 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 cyberthreats, and effectively secure critical assets and functions, cybersecurity teams and relevant medical staff should monitor official announcements for timely information on cyber risks relevant to healthcare sector. To maintain situational awareness, healthcare facilities can sign-up for, and regularly review, the following federal sites for up-to-date alerts and guidance:

- Health Sector Cybersecurity Coordination Center (HC3): Products
- HHS Healthcare and Public Health Sector: Highlights-Cybersecurity Edition
- HHS 405(d): Subscribe to The Post
- CISA: National Cyber Awareness System Bulletins/Reports; Sign-up for Alerts
- CISA: SHIELDS UP webpage
- CISA: Stop Ransomware webpage

To ensure readiness, healthcare facility information technology (IT) teams should incorporate basic IT preparedness principles into planning protocol, including:

- Understand historical and current healthcare-related attacks and their subsequent lessons learned.
- Know the vulnerabilities that face your organization and have a threat remediation plan.
- 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 use cyber hygiene services 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 that should be addressed.

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 can 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.
- ***Implementing effective cyber hygiene practices*** is critical to securing an organization's networks and resources. Healthcare facilities with limited IT resources—in particular smaller facilities—may explore free cybersecurity services and tools that are provided by federal agencies (e.g., the Cybersecurity and Infrastructure Security Agency [CISA]), and the public and private sectors. To help identify system vulnerabilities, evaluate resilience, and stay current on cyber practices, rural health centers can use specially developed toolkits for hospitals and clinics in remote settings.

Routine Mitigation

Facilities should establish regular vulnerability scanning and continuous monitoring practices to ensure the rapid identification of potential threats. As vulnerabilities are detected, they should be prioritized and remediated using patch management, blocking, and other practices that 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

- 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.

- Improve organizational security posture by remediating issues discovered during periodic ***penetration tests, vulnerability scans, and cyber risk assessments*** that are used to better understand potential threats and the overall integrity of the infrastructure. Ensure scans and penetration tests include operational and physical security technology.

- Ensure that threat remediation practices, such as ***patch management***, are properly vetted and consistently executed. Keep technology updated with the most recent patches as they are released; prioritize patches and updates for known vulnerabilities (e.g., legacy systems). Ensure exceptions to formal patch management policies are approved in writing. Implement a test environment to ensure patching and updates are done safely and with minimal impact to healthcare operations.

- Follow industry and federal guidance for ***system segmentation/partitioning*** where networks, functionality, and IT components are separated to control access and strengthen network security. Streamline data flow from interconnected systems to reduce system dependencies, promote faster recovery times, and reduce the number of affected systems.

- 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.

- Ensure mobile devices are protected by utilizing a mobile device management solution.

- Implement biomedical device security program that aligns with NIST and 405D.

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 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 state and local law enforcement, Federal Bureau of Investigation (FBI), and other federal, 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.
- Optimize planned outages to rehearse cyber loss plans and IMT response.
- Ensure emergency response planning ***includes representation from ancillary services*** and off campus locations, such as ambulatory, nutrition, 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 application***s 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. Integrate this potential situation into your organization business continuity planning.
- Communicate any emergency response changes to departments and relevant staff promptly.

Incident Reporting

- Consider the need to ***keep reporting threshold levels low*** as threats against healthcare systems continue to grow. Per federal cyber experts, facilities should be prepared to report any small/ unusual incident, or abnormal system behavior (e.g., unplanned, or seemingly random, shutdown/reboot/crash, service disruption, slow network).
- ***Report a cyber incident as soon as it is identified***, per CISA cyber experts who urge rapid reporting. Have a workflow/process in place to facilitate swift reporting. Ensure personnel across the health system understand, and are familiar with, how to report an incident, including who to report to, when to report, and what information to include. CISA provides details and guidance on incident reporting in their Cyber Event Information Sharing factsheet.

- Ensure health system ***cyber incident reporting policies comply*** with federal, state, or local reporting mandates. For example, when finalized, the Cyber Incident Reporting for Critical Infrastructure Act would require health systems to report a substantial cyber incident to CISA within hours.
- ***To report anomalous cyber activity and/or a cyber incident to CISA***, email report@cisa.gov or call (888) 282-0870. You may also report ransomware incidents via the CISA Incident Reporting System and/or through the FBI Internet Crime Complaint Center (IC3).

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.

*Based on processes used by Nebraska Medicine.

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 test and confirm that intended recipients have received critical communications (e.g., requiring a response back or ***read receipt***).
- Identify an ***out-of-band communication mechanism*** that can be used securely in the event of internal communication compromise.
- ***Have external communication templates*** prepared in advance that have been reviewed by external counsel and other necessary authorities.
- Have plan for ***providing in- and outpatients and their loved ones with situational updates and instructions*** where appropriate.

Insurance and Legal Considerations

- Ensure ***cyber insurance coverage*** is adequate for needs of the organization or facility. The Federal Trade Commission provides a downloadable cyber insurance checklist with general tips for finding the right type of coverage for your facility or health system.
- Understand when additional coverage may be necessary. While insurance may protect against general technology-related risk, ***expanded coverage may be needed*** 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 support services may be available, how to access them, and conditions of use.
- 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 insurance policy changes*** 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 compliance, or potential 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. Utilize the CISA Ransomware Response Checklist as a guide to inform potential ransomware response activities.

Vendors and Third-party Engagement

- Understand how ***vendor expertise and engagement*** affect the design, performance, and protection of critical system elements before, during, and after a cyber incident.
- ***Meet with vendors pre-incident*** to discuss how compromised systems or assets may manifest (e.g., inbound calls are interrupted but not outbound, disrupted functionality to life safety systems).
- 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.
- Consider ***joining trusted community threat information groups*** such as the Health Information Sharing and Analysis Center (H-ISAC) or an Information Sharing and Analysis Organization (ISAO) 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 using 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 to be prioritized during a recovery effort.
- 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 help an organization 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 event, a proactively completed ADM can outline where to assign resources and prioritize system restoration needs 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, as well as mapping applications and dependencies.

- Determine an application's restoration order during a disruption by ***ranking several operational elements***[2] to assess its impact on business processes and operations. If a system is affected by a cyber incident, identify 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 current protocol. The Homeland Security Exercise and Evaluation Program (HSEEP) provides guidance for developing, executing, and evaluating exercises that address preparedness. CISA offers a resource list of Tabletop Exercise Packages (CTEPS), that include a library of cybersecurity scenarios.

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 health system 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***, 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.
- ***Care providers, IT, emergency management, and biomedical representatives, vendors, and law enforcement should 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 who may be impacted by limited access to key technologies*** (e.g., computers, Internet, software applications) after a cyberattack. Include them in drills to determine equipment and supply needs to ensure continued operations; identify and resolve workflow issues.

Exercise Promising Practices

- Hospital leadership and managers should ***regularly review exercise 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.

- ***Have a comprehensive plan.*** This plan should be revised after usage for planned and unplanned outages and reflect lessons learned from each as well as from other expert sources.

- ***Know your plan.*** Understand requirements of the IMT structure. Determine who will fill each role. During a wide-scale cyber incident, IMT expertise is critical to the successful management of prolonged response efforts.
- ***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 the need to re-distribute essential roles among staff as they are moved to different departments to support altered clinical operations. Consider the need to establish downtime teams during the response effort to help implement forms and protocol.
- ***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 the amount needed. Know 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; supply ordering, pharmaceutical, lab 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 more than three days. Determine the amount of time that will trigger extended downtime processes to be activated.
- 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.
- ***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).

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 unavailable in different scenarios?
  - » Who can be redeployed to provide needed administrative or operational support?
  - » 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). Anticipate need for staff supplementation during recovery to lessen need for those providing bedside care having to balance with documentation “catch up.”
- 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*** and, 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 ***hiring and onboarding*** (e.g., orientations, personnel evaluations, licensing) during an extended downtime response.
- Identify standard work processes/operating procedures that will need to be adjusted to support staff.

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

Hospital Downtime Preparedness Checklist

Hospital Downtime Operations Checklist

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*** and identify a lead 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 operations and maintain safe patient care. The following steps can help ensure a smooth initial response:

- Rapid reporting of an incident to proper authorities (e.g., CISA, FBI) will enable prompt provision of ***federal, state, and local support/response services*** to an impacted facility.
- The IMT (or a similar counterpart) will ***determine the scale of an event*** to initiate and manage the correct response. These efforts should be based on pre-determined severity/impact definitions.
- The level of system downtime will correlate to the scope of impact on the 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.
- Include ancillary representatives and partners in all aspects of the response effort.
- 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.

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.*** Involve 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 any 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 extenuating circumstances (e.g., 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. Determine a cadence for routine updates.

- Recognize that the ***IMT structure may be modified*** as response efforts change due to evolving response objectives and operational needs. Establish operational periods to cover the response and IMT personnel for each time period.

Workforce Resilience

Departments and facilities may require additional (or reallocated) staff during downtime. Proper human resource and compensation policies should be put in place to readily accommodate the need for altered work schedules or staffing needs. Workforce leadership should conduct a real-time inventory of available staff to plan for possible redistribution of resources in different departments. Other steps that can bolster workforce resilience include:

- ***Continuously communicate the scale, expected duration of downtime, and pertinent instructions*** to staff so they can plan and react accordingly. When staff understand the severity of a cyber event and the plan for responding to it, 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 response staff*** early that may need to work altered or extended schedules. Plan for 24/7 work periods for critical recovery personnel. Consider their personal support needs (e.g., childcare, nutrition, lodging).

- ***Transition staff*** from departments with decreased resource needs/services to areas that require supplemental staffing (e.g., nurses can be moved from a surgical unit to assist with ED activities).

- ***Ensure workforce transferred to assist with recovery efforts have the necessary skillsets***. They should be familiar with the software applications and operational workflows within the department or have a training plan established.

- ***Implement proper orientation, mentoring, and/or supervision*** before re-deploying staff to new areas to ensure patient safety and effective job performance. Specific tasks should be identified and briefed prior to the transition.

- ***Identify senior staff that can provide additional downtime training***. Organize sessions for efficiency and 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 during a cyber incident. The health system IMT should continuously estimate downtime timelines and adjust response procedures as needed.

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.
- ***Implement a downtime team***—familiar with the process—to support staff during the time-consuming distribution and implementation of downtime documents.
- ***Verify that downtime documents being used are current***; if new forms need to be generated, ensure they go through proper approval channels.
- Ensure that when filling out forms, writing is legible, and information provided is compliant and contains all necessary data points.
- ***Consider security requirements for records, files, charts, 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***/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 communication***, 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 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, or transfer/exchange of support staff.
- ***Identify departments that may need additional support for new staff*** unfamiliar with manual operations, paper charting, downtime procedures; provide these departments with additional training/response support. Provide downtime example forms, resources (e.g., how to write safe clinical orders for medication/therapy).
- ***Plan for clinical and medical informaticists to be in the facility to staff help desks and/or round on units or offices to monitor situational response, mentor staff, and resolve local issues.***

Personnel Adjustments

- Consider how to ***use employees that are unable to work*** due to downed computer systems/technology. Ensure it is within the confines of labor, union, employment laws, and staffing or human resource policies.
- ***Designate personnel on the floor*** to identify resource gaps (who needs help, what are the specific tasks, resources required) 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).

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.
- ***Train providers in how to "write" orders when electronic health records are not available***.
- ***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.
- ***Reinforce the use of patient identifiers*** (primarily name and date of birth) on all documents and interactions.
- ***Encourage a "read-back" process*** as staff will rely more on the verbal transfer of information.
- ***Create workarounds in case of limited access to business continuity data*** and critical 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 workarounds.
- ***Document all cyber related recovery activities*** for emergency reimbursement (even if it is unclear what is allowable). Ensure personnel know what to document and how.
- ***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 incident 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.
- ***Consider whether the local HCC can/should be notified*** and if they are able to share incident information and alerts with their members.
- ***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. Transmit using the appropriate tool.
- ***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).
- ***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, "town hall" meetings, administrative rounding, 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 to establish 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.

The Cyber Incident Response Checklist can help healthcare facility personnel respond to an incident.

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 communication teams are aware of any information sharing limitations/restrictions.
- Be prepared to ***answer questions from the media, elected officials, regulators, and the public*** about the incident, and anticipate requests for information (e.g., is our data safe? Is your system safe?)
- Determine the need to ***establish regular communication with regulatory agency(s)*** (e.g., local health department, HCCs, The Joint Commission, CMS). Assign a point of contact to make expected updates.
- As a best practice in large-scale cyber incidents, ***consider avoiding media interviews***. Use exclusively written statements (at least at the onset of the incident) to control messaging and avoid 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, or to media outlets (or other public venues) where information can be exploited.
- Identify and ***use external advisors*** (aside from legal) to assist with media relations; leverage public relations networks to your advantage to control messaging.

Financial Promising Practices

- Have ***alternatives for providing financial counseling to patients*** while systems are down. Consider using pre-printed brochures; list helpful resources and organizations; or provide 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 issue***s 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 workarounds and avoid penalties.
- Dispatch financial ***staff to help monitor admitting, discharges, and transfers*** (ADT). Ensure patient registration and coverage information is correctly recorded.

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. Confirm personnel know the reporting protocol.
- Safety officers, patient advocates, and case managers should move to ***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***.
- ***Reach out to third parties by telephone*** to facilitate discharges to skilled nursing facilities to secure approval and plan accordingly.

Facility Security Considerations

During a cyberattack, normal security services will likely be altered or potentially unavailable. Changes to security protocol will need to be addressed immediately.

- ***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.
- ***Consider the following to address the need for additional officers/personnel*** (stationary vs. rounding) in special security/access restricted departments:
  - » 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 a 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.

RECOVERY

The System Restoration Checklist can help healthcare facilities ensure systems are restored after a cyber incident.

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.

- ***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 are brought back online.
- A determination may be made that ***some manually recorded data will not be reconciled*** with the EHR; instructions on what type of information this is and how it will be stored should be documented and shared.
- ***Some IT applications may be deemed non-recoverable***. In such cases, new alternative capabilities will need to be deployed.
- ***Workforce leadership will need to plan for mobility of staff*** and how they will meet workforce needs over an extended period of time. Consider the 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 is in the need-to-know group, 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.
- ***Integrate financial SMEs into recovery meetings*** to provide insight on timelines, manage expectations, and plan ahead for ongoing recovery efforts.
- When ***reconciling downtime charting/documentation***, HIM partnerships with compliance personnel and providers is important.
    - » While working to ***reconcile deficiencies in records***, start coding from paper charts while waiting for systems to be restored.
    - » Plan for the need to ***increase personnel numbers to perform coding***. Consider hiring vendors to assist.
    - » ***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 critical to avoid overburdening, and plan to wait a reasonable amount of time for signatures.
- Develop a ***financial policy to finalize record close-out***s if signatures cannot be verified. Use a stamp or authorized marking to identify records that have been audited, reconciled, and closed.
- ***Verify dates are correctly marked*** for revenue integrity. ***Ensure consistency in the charge entry process*** for any manual entries that take place, and document the 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 statements, 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 updated in October 2022 and reviewed by: **Lisa Bazis**, MS, Chief Information Security Officer, Nebraska Medicine; **Craig DeAtley**, PA-C, Director, Institute for Public Health Emergency Readiness, MedStar Washington Hospital Center; **Garrett Hagood**, CISO, Coastal Bend Regional Advisory Council; **Mark P. Jarrett**, MD, MBA, MS, Senior Health Advisor, Northwell Health; **Wai-Ling Mui**, ICF Public Health Preparedness Analyst, Biodefense and Global Health Security Consultant; **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 & Informatics, Nursing Professional Practice and Development, Nebraska Medicine.*

*It was originally developed in 2021 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:**
  - » Cybersecurity and Healthcare Facilities (Webinar)
  - » Cyber Incident Lessons Learned Finance Section
  - » Cybersecurity TA Responses
  - » Cybersecurity Topic Collection
  - » Healthcare Cybersecurity Resource Page
  - » Healthcare System Cybersecurity: Readiness & Response Considerations (Presentation)
  - » Healthcare System Cybersecurity: Readiness & Response Considerations (Webinar)
  - » Exchange Critical Issues in Healthcare System Preparedness Cybersecurity
  - » Lessons Learned from the MedStar Health System Outage
  - » Paper Based Hospital Records When EHR are Inoperable
- **Association of Healthcare Emergency Preparedness Professionals:**
  - » Cybersecurity in Healthcare Webinar
- **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):**
  - » Bad Practices
  - » Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
  - » Cyber Hygiene Services
  - » Cybersecurity Quick Links
  - » Cyber Threats to the Healthcare Sector and No Cost Cybersecurity Services
  - » Known Exploited Vulnerabilities (KEV) Catalog
  - » Protective Security Advisors
  - » Sharing Cyber Event Information: Observe, Act, Report
  - » Stop Ransomware
  - » Ransomware Guide

  - » Remediate Vulnerabilities for Internet-Accessible Systems
- **Department of Homeland Security:**
  - » A Lifeline-Patient Safety and Cybersecurity
  - » Cyber Tabletop Exercise for the Healthcare Industry
  - » Homeland Security Information Network Mission Centers
- **Federal Bureau of Investigation**
  - » Internet Crime Complaint Center IC3
  - » FBI Field Offices
  - » InfraGard
- **Federal Emergency Management Agency: Incident Command System Resource Center**
- **Federal Trade Commission: Cyber Insurance**
- **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:**
  - » Healthcare and Public Health (HPH) Sector Cybersecurity Checklist
  - » Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients
  - » Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)
  - » Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM)
  - » Medtech Vulnerability Communications Toolkit (MVCT)
  - » Operational Continuity-Cyber Incident (OCCI)
- **HIPPA Journal: Healthcare Cybersecurity**
- **Indiana Government Cybersecurity:**
  - » Cybersecurity Training and Exercise Guide
  - » Emergency Response and Recovery
- **International Medical Device Regulators Forum: Principles and Practices for Medical Device Cybersecurity**
- **National Institutes of Standards and Technology: Computer Security Resource Center- Healthcare Projects, Events, News, Publications**
- **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**
- **Osterman Research. Cyber Security in Healthcare**
- **Ready.Gov:**
  - » Business Impact Analysis
  - » IT Disaster Recovery Plan
- **United States Congress:**
  - » S.3600 - Strengthening American Cybersecurity Act of 2022
- **University of Tennessee: How to Tell if Your System is Compromised**
- **U.S. Department of Health and Human Services:**
  - » ASPR CIP for the Healthcare and Public Health Sectors
  - » ASPR Critical Infrastructure Protection (CIP) Bulletin
  - » ASPR Healthcare Preparedness and Response Capabilities
  - » Breach Portal
  - » Health Sector Cybersecurity Coordination Center (HC3)
  - » Joint HPH Cybersecurity Working Group/405(d) Program
    - Health Industry Cybersecurity Practices

APPENDIX: HEALTHCARE SYSTEM CYBERSECURITY READINESS & RESPONSE CONSIDERATIONS

This appendix provides additional information regarding IT practices, resources, and guidance provided by ASPR TRACIE partners and cybersecurity experts outside of healthcare facility operational considerations.

Additional Security Considerations

- When thinking through healthcare cybersecurity protections, explore specific topics that include:
  - Defense in depth strategies.
  - Principle of least privilege.
  - Creation of sandboxes.
  - External security of inbound vendors and/or servers.
  - Vulnerabilities presented by aging equipment that can be compromised with inbound hacking if tethered to an external server for upload or download of information (where patches are unavailable for antiquated equipment or are too expensive for the remaining life of the device).
  - Systems within a hospital that are being monitored from external vendors, where the whole componentry could be a vulnerability.
- Follow the "3-2-1" rule to maintain security of backups: at least 3 copies on 2 devices with one offsite; ensure offline networks are segmented.
- Utilize Multifactor Authentication (MFA) throughout an organization for access protections.
- When assessments are completed to identify vulnerabilities, ***rank the identified risk vulnerabilities*** based upon impact to patient care and safety, protection and privacy of patient data, and then non-clinical business operations. Ensure ***scans and penetration tests*** include operational and physical security technology.
- Experts state that it is important to understand that in some cases, vulnerability scanning is limited, and penetration testing is appropriate in many cases. Additionally, vulnerability scans of medical equipment in clinical use may lead to adverse patient outcomes by causing the device to reboot or otherwise not behave as expected. Vulnerability scans should be coordinated with medical equipment servicing groups to occur regularly when the device is available due to periodic/planned maintenance.
- In reference to ***Zero Trust network architectures***, NIST notes that there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (i.e., enterprise or personally owned).
- Facilities should consider use of strong encryption at the enterprise level to further protect critical data.

- For more information on ***contingency planning*** as it relates to cybersecurity, the NIST Contingency Planning for Federal Information Systems document provides specific information on the purpose, process, and format for formal contingency planning within the IT sector.
- Carnegie Mellon University provides additional information on the risks associated with moving to the Cloud, or cloud-based solutions, in their resource ***12 Risks, Threats, and Vulnerabilities in Moving to the Cloud***
- Streamlining data flow from interconnected systems will create more predictable traffic flows for monitoring and comparison.
- Monitor network traffic to limit to necessary ports and protocols, and restrict communications to external end points, especially ones with historical high risk geographically.
- The Communications Security, Reliability, and Interoperability Council IV Working Group final report provides information on cybersecurity practices for protecting and insulating a system. Such practices can contain spread within a segment or enclave.
- When segregating life safety equipment, eliminate trust relationships between life-safety and corporate networks, especially for authentication.
- Facilities should have a complete ***Configuration Management System and Configuration Management Database*** (CMS/CMDB) of all networked devices, software entities, and their Network Interface Card (NIC) characteristics such as media access control (MAC) address, as well as the major software components on said device.
- Additional information on vulnerabilities and protection of software-based medical technologies and their impact to patient care can be found in the HSCC Medical Device and Health IT Joint Security Plan.
- Experts suggest working with the National Telecommunications and Information Administration (NTIA) and understand the Software Bill of Materials (SBoMs) to leverage these information sources to map Common Vulnerabilities and Exposures (CVEs) to medical equipment in order to understand current and future risk vectors.
- Many networked devices can function in a non-networked mode; however, they require the care provider to be local to the unit (e.g., Radiologist at the MRI). Consider what plans are in place for additional staffing to provide for local interaction with normally networked devices.
- In cases where custom developed applications are critical to a facility, experts suggest it is imperative to have a proper secure ***System Development Life Cycle*** (SDLC) for the development of safe applications.
- Consider vendor Virtual Private Network (VPN) access as a possible attack vector and align controls with best practices. There should be risk evaluations associated to this attack vector as well as monitoring of the VPN connections.

Communications

- The CISA Priority Telecommunications Services (PTS) provide organizations that meet critical infrastructure criteria with emergency contingency communications capabilities through three services. Government Emergency Telecommunications Services (GETS) provides a landline network contingency, the Wireless Priority Service (WPS) provides a wireless network contingency, and the third service, Telecommunications Service Priority (TSP), provides priority restoration for critical communication circuits and hubs, as well as relocation support when communications circuits require routing to new service or business locations.
- A facility should ideally be informing their local partners first through the healthcare coalition (HCC) as well as the state. Healthcare facilities should understand in depth the communication protocol between the organization and the HCC.
- A facility should consider having or educating a ***Public Information Officer*** on communicating with external partners about Cyber events.
- More information on out of band communication mechanisms that are considered for entities currently using IP networks for voice communications is available via the MITRE partnership network.

Partners and Information Sharing

- The Healthcare Sector Coordinating Council FAQ resource provides information about the goals of the council, which include "identifying major cybersecurity threats and vulnerabilities to the security and resiliency of the healthcare sector, and developing cross-sector policy and strategic approaches to mitigating those risks" and how to become a part of the ***Cybersecurity Working Group***.
- For additional information on becoming part of the IT-ISAC, visit https://www.it-isac.org/.
- For additional information on becoming part of the ISAO see the FAQ page or contact the DHS ISAO inbox at ISAO@hq.dhs.gov.
- For exercises and drills, include documentation for existing architecture including security protection and monitoring solutions, which will greatly assist in just-in-time training and response.

Policies

- To better understand cybersecurity risk as an ***enterprise risk management*** issue, reference information available in the NISTIR 8286A - Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM).
- Review the passage of HR 7898, the ***HIPAA Safe Harbor Bill***, an amendment to the HITECH act where HHS is directed to provide regulatory relief and considerations for HIPAA covered entities which have met recognized cybersecurity practices, such as NIST and 405d.
- Information on the Health Industry Cybersecurity Practices (HICP) can be used to understand how HICP analyzes cybersecurity threats and vulnerabilities that could affect the health sector. Specifically, the HICP covers five threats and provides ten mitigation practices for industry.

- The HHS Incident Reporting, Policy and Incident Management Reference lists policies, guidance, additional incident management resources for reporting a cyber event.
- The CMS Information Security and Privacy Overview provides specific guidance for reporting an incident involving ***CMS information or information systems***.

Response and Recovery

- In cases where a healthcare facility may stand-up an Operations/Command Center in response to a cyber incident, they should closely review the FEMA Incident Command System Resource Center and National Incident Management System (NIMS) resources.
- Understand the role of cyber incident forensics firms, explore what companies in the area may offer necessary services and/or discuss options with the facility cyber insurance provider.
- Emphasis should be placed on testing backup RTO and RPO objectives. Understand that it is difficult to test full system restores from backups because of disruption to patient services. Experts suggest maintaining separate and secure copies of interfaces and application images.
- In terms of response, it is important to differentiate between eradication of the threat actor and restoration of services as both are critical steps. A significant number of intrusions restore services without effectively removing the threat, resulting in either an on-going cycle of compromise, or having a dormant threat remaining on the network.

Training and Personnel

- New cybersecurity threats are constantly appearing. The personnel entrusted with detecting cybersecurity threats need continual training. Training increases the likelihood of detecting threats and responding to threats in a manner consistent with industry best practices.
- Cybersecurity tools are only as good as the people reviewing the tools' results. It is important to ensure staff are able to identify the proper tools for an organization, recognizing it can take a significant amount of time to learn a complex organization's enterprise network. This makes retaining skilled personnel as important as acquiring them. While there is no perfect answer to stopping cybersecurity threats, ensuring knowledgeable IT personnel are on the team is critical to reducing cybersecurity risks.

Terminology

- ***Golden Images*** are a type of secure baseline disk image that is used as a template for systems to ensure consistency and ease of deployment with a high quality/high standard copy or backup. ***External Mirroring*** is the practice of data separation/redundancy. The practice entails having a "mirror" of critical data outside of the organization (offsite).
- In cybersecurity, ***threats*** differ from ***vulnerabilities***. Threats are intentional actions by a malicious actor. Vulnerabilities are weaknesses caused by a victim knowingly or unknowingly.
- ***Downtime*** is a term used by the IT industry to identify the time when a computer system, server, or network is unavailable or offline. For the healthcare industry this term means the time when a necessary piece of technology required for healthcare operations is unavailable resulting in the need for alternative workarounds to be established. Many times, this can mean moving to manual processes such as paper charts and dictation of medical procedures and treatment.
- ***Risk-based decision making*** in cybersecurity is an important component of understanding a facility's vulnerabilities and deciding on best strategies for protection or mitigation. The CISA Risk-based approach to National Cybersecurity resource can provide guidance to properly assessing and reducing risk.