CYBER DISRUPTION TOOLKIT

Guidance for Hospitals to Develop and Implement Strategies to Mitigate Cyber Disruption Impacts

Greater New York Hospital Association

Contents

Introduction

This Cyber Disruption Toolkit will help hospitals develop and implement strategies to mitigate cyber disruptions at their institutions. Innovation and technology have transformed how patient care is provided, whether at the bedside or via telemedicine. Cutting-edge care dependent on technology exposes crucial vulnerabilities that can bring patient care to a standstill.

Cyber disruptions have become increasingly prevalent in all industries, with health care being one of the major targets of cyber criminals. Hospitals remain vulnerable to cyber disruptions, including deliberate attacks on organizations, which cause technology to fail. Despite these challenges, hospitals prioritize preparedness to ensure that the core functions of providing patient care can continue following a cyberattack.

This toolkit provides guidance and best practices to help emergency managers, hospital operations staff, clinical leaders, and information technology (IT) professionals prepare for, respond to, and recover from a cyber disruption. Focused on the continuity of patient care operations, the toolkit highlights relevant IT, legal, and regulatory resources.

ACKNOWLEDGEMENTS

GNYHA formed an interdisciplinary internal committee in 2016 to address the cybersecurity needs of our members. We have worked with Federal, State, and local government partners to provide education, resources, and advocacy to our members. This toolkit stems from years of internal effort by GNYHA's Cyber Committee and Emergency Preparedness team and is informed by the knowledge and experience of our membership.

The toolkit also draws on the expertise and experience of hospitals including Hospital for Special Surgery, Memorial Sloan Kettering Cancer Center, NYC Health + Hospitals, NewYork-Presbyterian Hospital, Northwell Health, NYU Langone Health, One Brooklyn Health, The Brooklyn Hospital Center, Yale New Haven Health, and the University of Vermont Medical Center.

GNYHA is grateful for the support of our Federal, State, and local partners, including the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), which have provided expertise, information, and background for this toolkit.

As the cyber landscape continues to evolve and challenge us, we thank our partners for helping to ensure our hospitals remain resilient, prepared, and focused on their core mission, which is to provide timely, high-quality patient care to their communities.

HOW TO USE THIS TOOLKIT

This resource should supplement established emergency operations plans. It can be modified to your organization's size, resources, complexity, and capabilities.

The toolkit comprises four main sections: background on cyber disruptions and cyber attacks, preparedness steps your organization can take during normal operations, considerations during a cyber disruption response, and recovery actions. You will find the following features throughout this document:

CALL-OUT BOXES

Call-out boxes are used to supplement the information provided.

CASE STUDIES

Case studies provide real-world examples to illustrate the information provided.

TEAR-AWAYS

Templatable documents can be used as "tear-aways" and added to your organizational plans. Where possible, links to editable documents are also included.

ADDITIONAL RESOURCES

Hyperlinks are provided for additional resources that expand upon concepts in the toolkit.

Important Terms and Definitions

- Downtime: Planned or unexpected events when a technology system is unavailable or fails to perform as designed.
- Cybersecurity Event[1]: An event that has been determined to have impacted an organization, prompting the need for response and recovery.
- Cyber Attack[1]: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
- Cyber Disruption: Used to categorize any interruption or disruption of technology, whether malicious or non-malicious, occurring at a health care facility.

Cyber Disruption Threat Profile & Background

Health care organizations—due to their reliance on technology and the high monetary and intelligence value of their data—are targets for cyber disruptions. Targeted data attacks can expose valuable information, including patients' protected health information (PHI), financial information (e.g., credit card and bank account numbers), personally identifying information (e.g., Social Security number), and intellectual property around medical research and innovation.

Terrorist organizations, cyber thieves, and state actors can carry out cyber attacks. Political conflicts abroad can increase the threat of cyber attacks, particularly from state actors that are adversarial toward the United States. In 2023, the Department of Defense (DOD) identified the People's Republic of China, Russia, North Korea, and Iran as countries with current political conflicts that pose a cyberthreat against the US. Organizations should monitor threats to critical infrastructure from state actors.[2]

TRENDS IN RANSOMWARE ATTACKS ON US HOSPITALS, CLINICS, AND OTHER HEALTH CARE DELIVERY ORGANIZATIONS, 2016–21[3]

Ransomware attacks have **more than doubled** from 2016 to 2021 (43 to 91)

PHI exposure increased 1.3 million (2016) to **16.5 million** (2021)

44.4% of health care delivery organizations that experienced a **ransomware attack** had disruptions in care delivery

The increase in the number of attacks that were reported very late **are exceeding the statutory limit of 60 days** from the attack

From **2016 to 2021**, the number of ransomware attacks that resulted in some or all the stolen PHI being made public increased

Main Cyberattacks and Vectors Facing Health Care Facilities

Common Types of Cyberattacks	
Ransomware	Malicious actors use ransomware attacks to effectively "lock" an institution's IT system, preventing users from logging into applications or workstations, rendering technology useless until a ransom is paid.[4] This type of attack has the biggest impact on patient care. Among health care organizations that experienced a ransomware attack, 68% said it disrupted patient care, with 59% of those respondents saying it resulted in delays and procedures that resulted in poor health outcomes.[5] Twenty-eight percent of respondents from organizations that experienced a ransomware attack said it caused a rise in the patient mortality rate.[5] More than 70% of successful cyberattacks on health care organizations in the previous two years were ransomware attacks, according to a 2019 report.[6] *Example: The University of Vermont Medical Center cyberattack in 2020.*
Denial of Services (DoS)	DoS attacks involve malicious actors sending a massive number of individual requests to an institution's servers, such as their website, overwhelming the system and resulting in near-impossible use of the system. DoS attacks account for 48% of cyberattacks.[7] *Example: Boston Children's Hospital Cyberattack 2014*
Vectors and Mechanisms for Malicious Attacks	
Social Engineering (e.g., Phishing)	Phishing is a cyberattack that involves sending a message, usually via e-mail, to employees. Social engineering—or the manipulation of an individual's online behavior—is exploited to influence at least one of the recipients to open the message and either navigate to a website or download a file that has been rigged with malware.[7] Often, e-mails resemble an official notice from an institution or may look like they were sent from a colleague. The sender may also be trying to influence the recipient to reply with confidential or sensitive information or to take actions such as changing payment or payroll information or resetting or sharing passwords to benefit the threat actor. Social engineering attempts can lead to cyberattacks such as DoS and ransomware.
Network-Connected Medical Device Infiltration	Outdated medical devices that lack security patches can be leveraged to access an institution's network or to provide false medical information. While unsecure medical devices are among the top threats facing health care organizations' cybersecurity posture, only 51% of organizations say their cybersecurity strategy includes prevention and response to an attack on network-connected medical devices, according to a 2023 survey of health care organizations.[5]
Accidental or Malicious Insider Data Loss	Insider threats can be either unintentional or malicious and consist of employees, contractors, or other individuals who may have access to an institution's knowledge, databases, or systems. Of the data breaches reported as an insider data loss, 61% were primarily unintentional or caused by negligence.[8]
Loss or Theft of Equipment or Data	This is another form of insider threat, 25% of which resulted in stolen credentials due to worker negligence.[8]

IMPACTS ON PATIENT CARE

Patient safety and care delivery are key concerns during cyber disruptions.[9] Cyber disruptions that disrupt access to medical records and the operation of critical medical devices and other technologies can hinder a hospital's ability to effectively provide patient care. Bad actors seeking to steal private patient data can also alter said data—intentionally or unintentionally—which could seriously impact patient health and outcomes.

In a Ponemon report on the impact of ransomware on patient safety, **53%** of respondents from health care organizations said that a ransomware attack disrupted patient care, and **45%** of respondents said that ransomware attacks caused complications in medical procedures. **70%** of respondents reported that a ransomware attack caused an increase in ambulance diversions. Finally, **21%** of respondents stated that ransomware had a negative outcome on patient mortality rates.[10]

CASE STUDIES

Burlington, Vermont – University of Vermont Medical Center

The University of Vermont Medical Center experienced a cyber attack in 2020 that greatly impacted services across the hospital. The attack caused the oncology department to see a 41% decrease in total outpatient visits. In the first week, 63% of the facility's infusion center visits dropped (before rebounding steadily over the following weeks).[11] Notably, a study found that there is an increase in mortality when there was a treatment delay of four weeks.[12]

Düsseldorf, Germany – Düsseldorf University Hospital

In 2020, a 78-year-old woman suffering from an aortic aneurysm was being transported to Düsseldorf University Hospital when a ransomware attack caused the ambulance to divert to a hospital further away. The delay in receiving lifesaving treatment resulted in the woman's death before arriving at the hospital.[13]

Mobile, Alabama – Springhill Medical Center

Springhill Medical Center experienced a 2019 ransomware attack that impacted hospital operations.[14] A subsequent lawsuit alleged that a pregnant patient's baby died because the ransomware attack disrupted many vital hospital operations during labor and delivery. Specifically, the lawsuit alleged that fetal tracing information was only available at the patient bedside and not remotely at the nurses' station.[15]

FINANCIAL CONSEQUENCES

Stolen health records can be worth up to 10 times more than stolen credit card data on the dark web. The cost to address a health care breach is almost three times that of other industries—averaging $408 per stolen health record versus $148 per stolen non-health record.[9] Overall, a single cyber attack can cost a health care organization more than $10 million.[17]

Cyber disruptions can impact a hospital's revenue cycle. A 2021 cyber attack against Scripps Health in California that disrupted patient care resulted in an estimated $90 million in lost revenue.[18]

Two factors that can severely impact hospital revenue during a cyber disruption are 1) decreased patient volume and elective surgical procedures and 2) inability to recoup care costs from insurance payers.

RANSOMWARE ATTACK ASSOCIATED WITH DISRUPTIONS AT ADJACENT EMERGENCY DEPARTMENTS IN THE US[16]

Ransomware attacks not only negatively impact the targeted hospital, but also adjacent hospitals:

127.8%

increase in visits where patients left without being seen

47.6% increase in median waiting room times

35.2% increase in mean ambulance arrivals

50.4% increase in visits where patients left against medical advice

6.7% increase in mean admissions

REPUTATIONAL HARM

Cyber disruptions can have a lasting impact on a health care facility's reputation. 83% of consumers said they would not patronize a business for several months after a cyberattack, with 21% saying they would never return to the business.[20]

Harm to a hospital's reputation can be compounded if PHI is compromised, which can also lead to lawsuits, as seen in the aftermath of the 2021 Scripps Health cyber attack.[21]

CASE STUDY

Spring Valley, Illinois – St. Margaret's Hospital

The financial impacts of cyber disruptions on health care organizations have led to bankruptcies and closures. St. Margaret's Hospital was forced to permanently close following a ransomware attack that delayed its ability to submit claims to insurers for months.[19]

Preparedness

Successful outcomes from a cyber disruption begin during the weeks, months, and years before it happens. Preparedness helps organizations to ensure that continuity gaps are addressed and patient care impacts are significantly minimized.

CYBER AS AN ORGANIZATIONAL-WIDE CULTURAL PRACTICE

Because cyber is an enterprise risk, a culture of cyber preparedness and mitigation is essential for a successful response to a cyber disruption and must be instilled across the organization. Typical cyber preparedness sits within an organization's IT team, which includes cyber hygiene practices such as multifactor authentication and phishing awareness campaigns. All levels of an organization, from frontline staff to the chief executive officer, need to understand the importance and implications of cyber hygiene. The preparedness practices below are critical steps to building your organization's resilience and require your leadership's buy-in.

High Reliability Organizations

The Joint Commission defines organizations that operate in complex, high-hazard domains for extended periods without serious accidents or catastrophic failures as high reliability organizations (HROs).[22] Characteristics of HROs include preoccupation with failure, reluctance to simplify, sensitivity to operations, deference to expertise, and commitment to resilience. Many hospitals already have developed programs to become HROs. Cyber disruption preparedness can be leveraged within this model, from leadership engagement to frontline staff. HRO initiatives are an advantageous model to use for preparedness efforts and can be an efficient mechanism for training (see page 14).

https://web.mhanet.com/media-library/high-reliability-organization-toolkit/

DEVELOP EXPERT TEAMS

The following "teams" were adapted based on the iDart Model, which was developed by Massachusetts General Hospital and via conversations with multiple GNYHA member hospitals.[23]

Disruptions can cause chaos in organizations, emphasizing the importance of clearly defined roles and responsibilities for staff to minimize confusion in the event of a cyber disruption. While the following teams with defined roles and responsibilities are noted for consideration, these functions should be embedded into existing quality and incident response structures, where possible.

Cyber Champions

During a cyber disruption, your organization's IT department will be spread thin working to bring multiple systems back up. To alleviate the pressure on IT personnel, your organization should establish "cyber champions" across both clinical and non-clinical teams. These individuals will bridge the preparedness and response gap between IT and the clinical workforce.

Cyber Disruption Incident Response Team

As an organization's initial response to a potential cyberthreat, the cyber disruption incident response team is immediately alerted to any IT outage. At a minimum, this team should consist of IT manager(s), IT clinical representatives, emergency manager(s), hospital administrator(s) on call (AOC), and nursing administrator(s) at affected hospitals. Health systems should adapt this configuration based on their corporate structure and determine the need for a corporate-level team and hospital-specific team. Initial impacts and concerns are defined by this group, which understands that impacts at facilities determine the need to escalate an incident to hospital administration and/or activate their command center and incident command system (see page 25). This team should align with existing emergency operations plans and be incorporated as appropriate.

Cyber Policy Group

An executive group must be engaged early during cyber disruptions to provide strategic direction on cyber policies. Organizations may have a pre-established executive team charged with decision-making on an emergency basis, which should be leveraged for cyber disruptions. This policy group should be kept to a manageable size to ensure effective decision-making and should include at a minimum the chief executive officer (CEO), chief information security officer (CISO), chief information officer (CIO), chief financial officer (CFO), chief operating officer (COO), chief communications officer, general counsel, and emergency management leadership. Alternate means of communication are crucial and could include providing home phone numbers and personal e-mail addresses. Your cyber insurance carrier may have additional resources that this policy group can leverage early in a response. This executive team should be integrated into your facility's incident management structure and connected to the incident commander/unified command.

Department Downtime Teams

Department downtime teams that are well-versed in all downtime procedures should be established for each department or unit. Department downtime leads should develop comprehensive planning for operational downtime procedures. Teams should be formed to address both the operational and IT aspects of downtime. The department downtime team should consist of staff and managers in the department and work closely with IT disaster recovery teams to develop, educate, and drill staff on downtime procedures (see page 14). Clinical departments should also include representatives from the patient quality and safety team.

NOTE ON IT TEAMS

IT teams have three core missions during an incident response:

- General IT Support—ensure technology works for the end user
- Disaster Recovery—scope and bring IT systems back online
- Forensic Investigation—understand the root issue of the cyber disruption, including determining if disruption is a cybersecurity issue

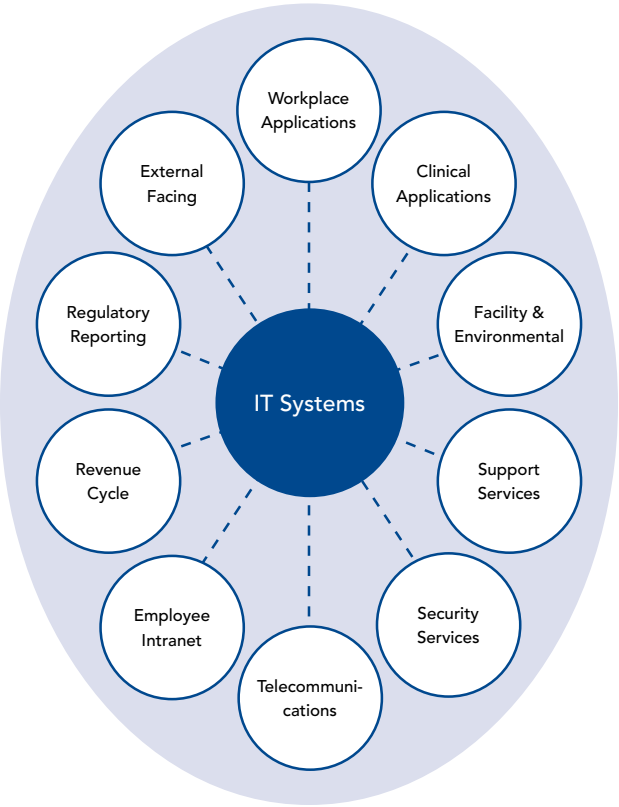
Your IT department may organize differently. IT departments must be engaged to understand the structure of their response and how to navigate it within your organization's incident management structure.

PREPARING FOR DOWNTIME

Departments and units should determine which devices are reliant on network and/or internet connectivity and educate staff about them. Workarounds should be developed prior to these devices failing. Recognizing the entire constellation of reliant devices, including non-obvious pieces of technology, is important. Evaluating core systems (see page 22) can provide further understanding of the entire scope of reliance.

Downtime procedures should be considered for every piece of technology that your organization uses.

Ensuring consistent processes at all affiliated facilities, campuses, and institutions can avoid discrepancies in recordkeeping and documentation and ensure competency among staff members. Downtime procedures should be developed at the highest practical level (e.g., nursing department develops downtime for infusion pumps, intensive care unit [ICU] develops downtime for extracorporeal membrane oxygenation).



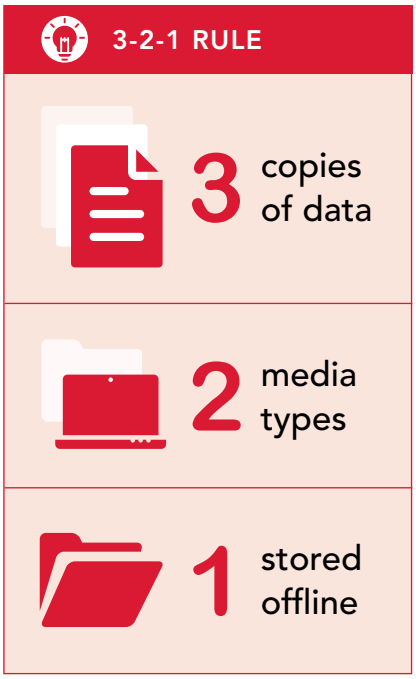
Critical Data Backups

Organizations rely heavily on data for their everyday operation whether they are using electronic health records (EHRs) to inform patient care or analyzing payer information to track revenue or time clock data for employee compensation. Data is an organization's critical backbone.

A significant cyber disruption such as a ransomware attack will lead to a considerably long outage. While

your organization may have prepared staff for planned downtime during maintenance or system updates that often take hours, when an outage is extended to weeks and months, it is important to prepare differently.

All areas of your organization should implement the 3-2-1 rule for crucial data, which calls for three copies of data to be retained on at least two different types of media—with at least one of them stored offline.[24] While your IT department's practices could include backing up data, offline and analog backups should be kept at a department level to ensure quick access, particularly as IT staff may be unavailable for individual department requests.



All units should have access to a downtime computer, which provides an offline copy of patient records for reference. Staff should maintain competency and ensure regular IT training on how to access and use these computers in case of a disruption. Planned downtime for regular system maintenance is an ideal opportunity to maintain staff competency in backup technology.

Health Information Exchange

EHRs are often the first systems to be impacted during a cyber disruption, bringing normal operations and patient care to a halt. While offline backups of patient records are critical, if a downtime computer is not operational or a patient's chart is inaccessible, your region or state's health information exchange (HIE) may be able to provide patient-specific information. Organizations should understand how to access and use HIEs to access pertinent health information as part of their preparedness efforts.

Statewide Health Information Network for New York (SHIN-NY)

New York State's SHIN-NY is the statewide HIE, which facilitates the secure electronic exchange of patient health information among health care organizations.[25] While this is an important resource, it is not the be-all and end-all. For the most part, qualified entities (QEs) maintain only a snapshot of a patient's record, called the consolidated continuity of care document (C-CDA). The C-CDA comprises certain structured data elements that are necessary for continuity of care, such as information on medication, vital signs, and immunizations. Although limited, the C-CDA could provide some information that may be helpful to the continuity of patient care during a cyber disruption.[26]

New York State's QEs are listed on the following page. Determine which QEs your organization belongs to and the primary contact from your organization. Your organization may participate in multiple QEs depending on each individual facility's location. Whether or not you rely on a QE during downtime, you should contact your QE if you experience a cyber disruption incident due to your organization's connection to the QE's system. Organizations should review their participation agreements with their QE for any requirements related to reporting and coordinating the response to security incidents.

NEW YORK STATE QEs

- Bronx Regional Health Information Organization (RHIO): https://bronxrhio.org/contact-us/
- HealtheConnections: https://www.healtheconnections.org/contact-us/
- HEALTHeLINK: https://wnyhealthelink.com/contact/
- Healthix: https://cx.healthix.org/contact
- Hixny: https://hixny.org/contact-us/
- Rochester RHIO: https://rochesterrhio.org/contactus

HEALTH INFORMATION EXCHANGE PLATFORMS OUTSIDE OF NYS

- New Jersey Health Information Network: https://www.njii.com/healthcare/new-jersey-health-information-network-njhin/
- Connie (Connecticut HIE): https://conniect.org/
- CurrentCare (Rhode Island HIE): https://riqi.org/solutions/health-information-exchange/currentcare/
- PA Patient & Provider Network (Pennsylvania HIE): https://www.keyhie.org/products-services/pa-patient-and-provider-network-p3n
- eHealth Exchange (National HIE): https://ehealthexchange.org/

CLINICAL PREPAREDNESS PRACTICES

Clinical leadership should evaluate and determine the most critical functions and services of their respective departments that will be impacted by a cyber disruption. In other words, the systems that—if you operate without them—could potentially jeopardize patient care quality. Using an evaluation process with help from the department downtime team, clinical units should develop a comprehensive list of critical functions and services and develop workarounds and solutions for such technologies.

Clinical teams should consider the following to aid in patient safety during a cyber disruption and downtime:

- Catalog up-to-date critical medical guidelines and clinical reference materials to be accessible during downtime
    - EHR provider alerts such as protocol considerations and pharmaceutical cautions, which are typically embedded in EHRs, may be disabled. Considerations for additional manual safety checks should be made via peer-provider review or a designated safety officer for high-risk procedures or critical patients.

- Create a downtime box or cart for each department to be deployed to a centralized location within the department. Ensure staff know where the box or cart is located and how to use it. The box could include:
    - Downtime forms, which mimic the format of EHR questions and ensure ease of use. Maintain these downtime forms and plans on multiple platforms (intranet, thumb drives, in print, offline).

  - Portable radios to assist communication on a patient floor. Low-cost, short-range technology solutions, including commercially available push-to-talk radios, should replace clinical mobile companions and other app-based communication.
  - Essential printed reference information, quick-start cards, checklists, and key instructions, including patient treatment protocols
  - Other supplies such as paper, pens, folders, and binders

- Develop reminders for standardizing recording procedures and medications (e.g., dates should be date of service, not date of entry)

- Review transfer plans and agreements with other facilities for patients who require services that are impeded by non-working technology, particularly patients requiring offline radiology services, and identify a process to transfer medical records and/or essential documents. Identify a member of senior staff who can assist new residents and nurses with manual charting procedures.

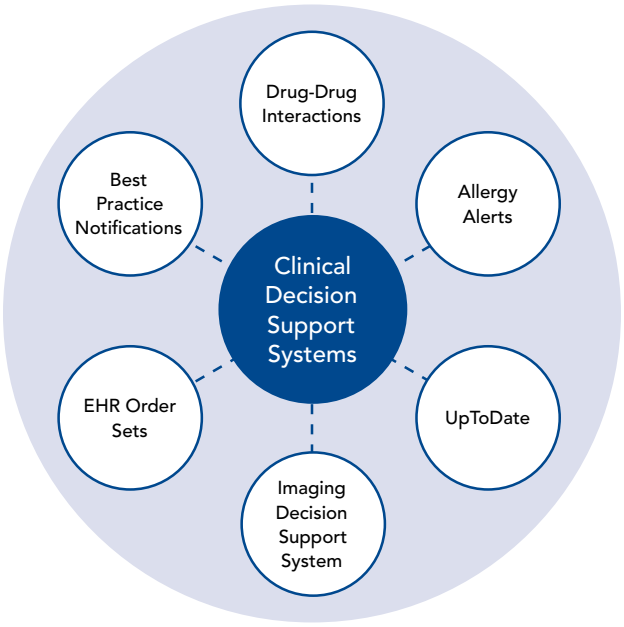
- Develop staff and clinical provider contact lists that are continuously checked and updated

- Evaluate existing downtime procedures to ensure they cover extended downtime periods and highlight differences in procedures for unplanned and planned downtime

Focus on Clinical Decision Support Systems

Clinical Decision Support (CDS) systems, which are integrated into a hospital's EHR, provide real-time information to best inform patient care.[27] Examples of CDS systems include drug-drug interaction (DDI) alerts, imaging decision systems, and EHR order sets.[28] Recognizing that there are many support systems and that a cyber disruption could make these systems inaccessible, hospitals should determine which of these systems are vital to patient safety and have them accessible in paper forms.

DDIs are a common EHR alert that providers see daily. The Office of the National Coordinator for Health Information and Technology (ONC) developed a comprehensive list of critical DDIs that hospitals can implement into their EHR with the goal of having these critical DDIs as a foundational baseline.[29] Level 1 alerts—which consist of the most serious, life-threatening interactions implemented as "hard stop" alerts that require a clinician to either cancel the order they are writing or discontinue the preexisting, interacting medication order—were used to determine this list.



UpToDate is a type of CDS platform that gives precise and timely information to help providers make specif-

ic recommendations for diagnosis, management, and treatment. UpToDate is one example of an outside CDS that could be integrated into your EHR.[30] While UpToDate can be accessed without an EHR, other access points to the system may not be common practice at your organization. Login credentials to access this resource outside of an EHR should be a typical downtime practice if your organization uses UpToDate as a common CDS system.

DOWNTIME FORMS AND REFERENCE DOCUMENTS

Downtime forms ensure continuity of operations for both clinical and business practices.

Clinicians largely record activities—including patient assessments, physician orders, medication orders, and other required documentation—through EHRs. While EHR providers may have and provide downtime forms, it is often an optional service. Organizations should review their contract language and discuss available solutions with their EHR provider.

Having hard copies of the following forms and references is recommended.

Department	Downtime Form
Clinical	• History, physical, and progress notes • Patient medical history • Medication & allergy list • Laboratory orders • Pharmacy & prescription orders • Radiology orders • Flowsheets for patient vitals • Patient safety & time-out checklists • Patient treatment protocols • EHR-driven best practice alerts
Patient Access/Admissions	• New patient registration forms • Patient demographic face sheet • Appointment schedulers
Finance/HR/Supply	• Patient billing form • Employee timesheets • Inventory list of current supplies • Employee & department expense form • Vendor/third-party supplier contact information • Supply chain order forms • ICD-10 code list
Legal/Regulatory	• External regulatory agency contacts • GNYHA reporting resource (see page 45)
Communications/Public Relations	• Internal department staff contact list

CORPORATE PREPAREDNESS PRACTICES

Corporate departments should leverage existing business continuity plans (BCPs) during cyber disruptions. All departments should consider the following steps when reviewing BCPs:

- Conduct vulnerability assessments across your organizations to head off potential attackers
- Develop messages for use during a cyber disruption. These messages should be preapproved by hospital administration and legal counsel (see page 40).
- Build procedures for personnel working extended shifts during a prolonged cyber incident
- Develop and have in place a business continuity of operations plan that will address all emergencies, including cyberattacks
- Review contract language with your EHR provider. This can detail what may happen to your EHR during a cyber disruption.
- Determine who in your organization will be the internal and external spokesperson during a cyber disruption

TRAINING AND EXERCISES

Training staff and conducting regular exercises are essential for effective cyber disruption response and building muscle memory. While many organizations require general cybersecurity hygiene for all staff (e.g., phishing awareness campaigns), departments must provide training on workarounds and downtime procedures for each staffer's specific job function.

LEARNING SERIES: CYBERSECURITY FOR THE CLINICIAN

The Health Sector Coordinating Council developed an on-demand video learning series for clinicians on various cybersecurity-related topics. The videos use non-technical language to explain how a cyber disruption could affect patient care and overall operations and how to keep data safe from potential attacks. This free series provides one continuing medical education/continuing education credit.

https://healthsectorcouncil.org/cyberclinicianvideos/

TOOLKIT: HEALTHCARE AND PUBLIC HEALTH CYBERSECURITY

The Cybersecurity and Infrastructure Security Agency (CISA) is a resource for every aspect of cybersecurity. In coordination with the Department of Health and Human Services (HHS), it released a health care and public health cybersecurity toolkit. This toolkit consolidates many of their resources and helps health care organizations improve their cybersecurity program.

https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare

Training Considerations

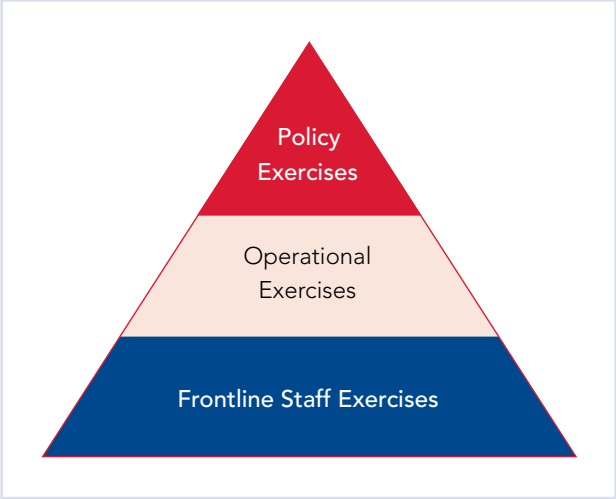
Considerations for implementing regular training include:

- Offer frequent training in downtime procedures to allow for continued competency
- Embed downtime training in new-hire and recurring training initiatives to reduce the burden on additional trainings
- Offer trainings during non-business hours for staff who work nights and weekends
- Provide in-person training to familiarize staff with locations of equipment (e.g., downtime computers), forms, and printed procedures

Clinicians rely on technology during patient care. Trainings should include clinical competencies for skills they may not practice regularly—such as auscultating blood pressure or monitoring cardiac telemetry—to ensure these procedures can be performed in lieu of network-connected medical devices.

Exercises

Exercises can identify gaps in cyber disruption plans and improve processes. Conducting exercises in a "no-fault" environment and using them to foster a learning environment is important. All levels of an organization's preparedness must be tested, from executive leadership down to the frontline staff level.



Policy Exercises

Executive-level engagement is crucial during a cyber disruption and can often set the tempo of a response. Tabletop exercises are an effective means to understand policies and decisions from leadership ahead of a cyber disruption. IT and the CISO should develop a plausible scenario for each exercise.

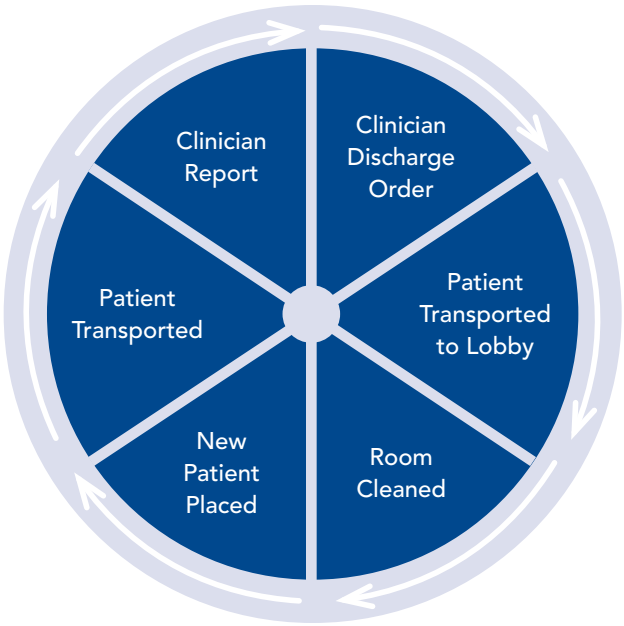
Policy exercises ideally include the CEO, CIO (including any chief medical information officer or chief technology officers), CISO, CFO, general counsel (including any external cyber legal counsel), emergency management, and the chief medical officer.

Topics to be explored should include:

- IT characterization of threat/impact of cyber disruption
- Notification of any cyberattack to relevant regulatory agencies
- Communication to staff, visitors, and patients
- Decision on ransomware engagement

Operational Exercises

Operational processes often cross many workflows, systems, and departments. Operational exercises with department leaders and representatives can be beneficial to testing these multifaceted processes.



Tabletop exercises can be useful, particularly ones that detail a specific process step by step. For example, the movement and placement of a patient into an inpatient hospital bed touches multiple departments and systems, often managed through an EHR or other software. Technological efficiencies are lost during a cyber disruption, requiring manual reporting of room and patient discharge status and whether the room has been cleaned for usage. Clinical reporting also may require a different approach without EHR access.

While individual departments could have downtime procedures for each of their roles, functions together may not work as planned. Exercises should not be limited to bedside patient care or specific business services, but should be exercised across departments that have co-dependencies. Simulating critical processes such as patient movement, which touch multiple departments, can ensure patients remain safe and that staff know about bed status.

Frontline Staff Drills

Muscle-memory maintenance among frontline staff is difficult, particularly in departments that have around-the-clock operations such as patient care units.

Incorporating exercises or drills into existing daily staff check-ins or regularly scheduled HRO huddles at the department or unit level can be most effective. These huddles can also be a way to conduct small drills with units about what could happen during a cyber disruption (plus other emergencies such as a power outage). Short scenarios can be written with follow-up questions for staff leaders to reinforce formal training.

TEMPLATE: PREPAREDNESS EXERCISES

GNYHA and CISA developed scenario templates that can be used as a starting point for your organization's exercises.

https://bit.ly/cyber-template

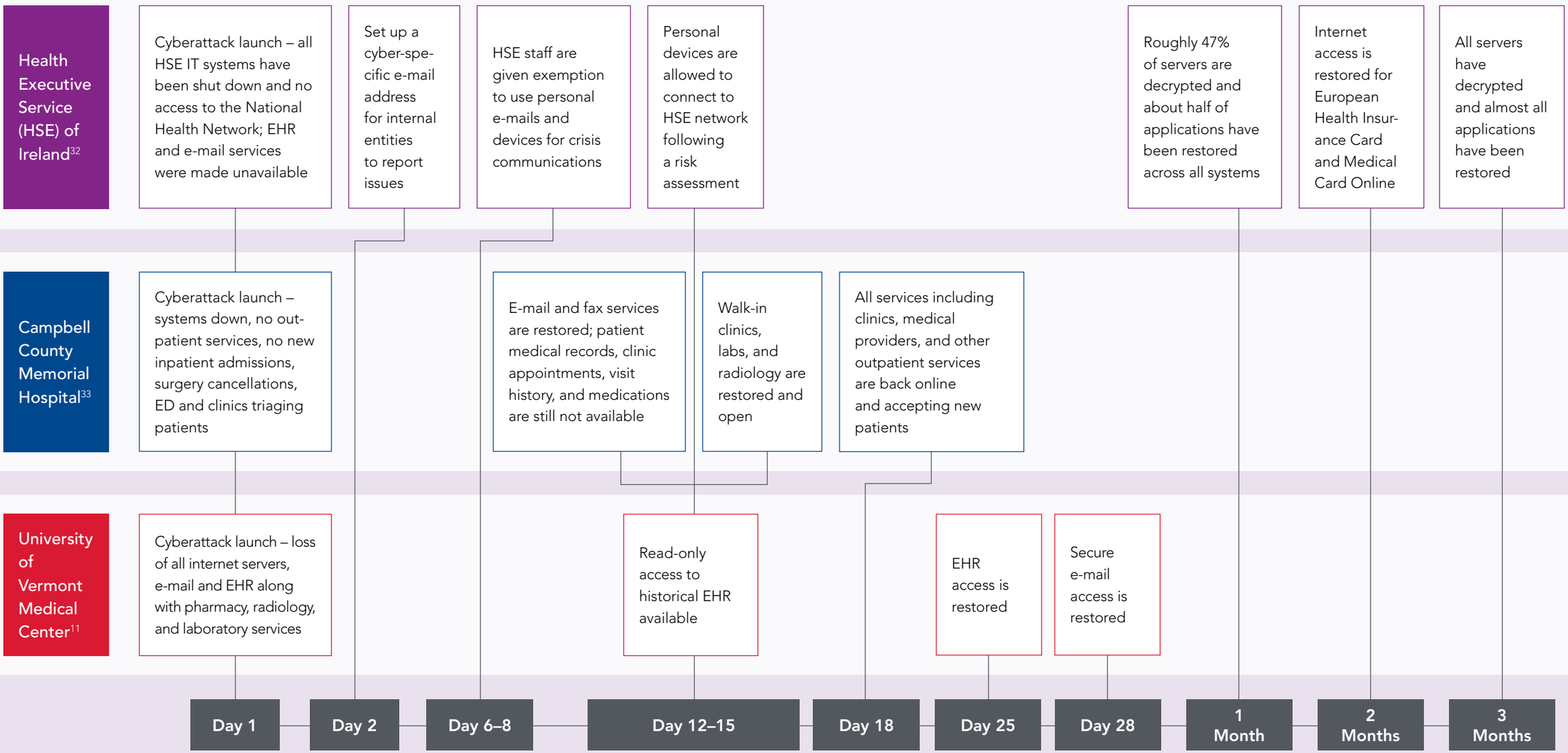
STAFF HUDDLE DRILL *SAMPLE*

Scenario: You are working on the patient floor when you go to document a patient order at your workstation. Your workstation seems unresponsive, and your attempt to use another gives the same result. You quickly report this to your supervisor, who just received word that all systems are down and tells you to revert to downtime procedures.

- What resources are available on the unit/in your department that you can use during downtime (e.g., downtime box, downtime computer, manual forms)?
    - Where are these resources physically located?
- Besides your workstation, should you check any other critical equipment?
- Are there departments that you need to contact to continue your work?
- What are you communicating to patients and their families (if applicable)?
- What changes if systems remain down for 12-plus hours?

Debrief and discuss these questions, identifying any areas for improvement, including follow-up training or orientation to downtime resources.

Case Study: Comparative Timeline for Cyberattacks



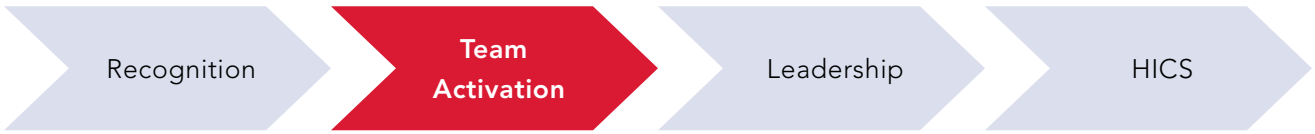
Response

RECOGNITION AND NOTIFICATION

Initial responses to cyber disruptions set the pace and structure for how your organization manages the consequences and recovers from disruptions in business operations. Recognizing an incident early, characterizing a disruption, and convening key leaders are critical to success.

Convening groups may be difficult given the scope and severity of the disruption, particularly if normal communication mechanisms fail. In-person groups may be more effective, but organizations could contemplate using encrypted virtual platforms. Consult with your IT department on which platforms are encrypted at your organization. Organizations should also maintain more basic communication venues that do not require internet connectivity, including wireless connections such as telephone conference call bridges (see page 38).

Initial Recognition of Incident



When a cyber disruption of any scale has been confirmed, the cyber disruption incident response team should be convened immediately. This group should work to determine the scope of the disruption and impacts on hospital systems, functions, or services. Recognizing the on-call nature of some team members, messaging channels, conference calls, or other remote capabilities may be the most effective way to communicate. Decisions on escalation due to the disruption should be made rapidly.

Team Activation: Cyber Disruption Incident Response Team

The cyber disruption incident response team should convene to discuss impacts to operations when an incident has happened (see page 8). The conversation should include the following individuals:

Title	Name and Contact Information
IT Downtime Manager	Name: _____ Primary Phone Number: _____ Secondary Phone Number: _____ E-mail: _____
Emergency Management Manager	Name: _____ Primary Phone Number: _____ Secondary Phone Number: _____ E-mail: _____
Hospital Administrator on Call	Name: _____ Primary Phone Number: _____ Secondary Phone Number: _____ E-mail: _____
Nursing Administrator Lead	Name: _____ Primary Phone Number: _____ Secondary Phone Number: _____ E-mail: _____
Clinical IT Representative	Name: _____ Primary Phone Number: _____ Secondary Phone Number: _____ E-mail: _____

Questions for the group:

- What is the scope of the incident?
- Is this disruption isolated or are there widespread impacts?
- Have hospital operations been impacted?
- Can this disruption be handled using the resources provided by this group?
- Which departments should you discuss the disruption with?
- Should we tell departments to shift to downtime procedures?
- Should we engage hospital leadership?

Hospital Core System Status Checklist

Workplace Applications

- [ ] E-mail and Word Processing
- [ ] Phone Lines
- [ ] Radios & Repeaters

Clinical Applications

- [ ] Electronic Health Records
- [ ] Laboratory Software
- [ ] Radiology (CT, MRI, PET) Software
- [ ] Workstation on Wheels
- [ ] Point-of-Care Devices
- [ ] Telemetry Monitoring
- [ ] Translation Service
- [ ] Consult Telemedicine

Facility & Environmental Applications

- [ ] HVAC
- [ ] Temperature Control Monitoring
- [ ] Pneumatic Tube System

Support Services

- [ ] Supply Dispensing Machines
- [ ] Pharmaceutical Dispensing Machines
- [ ] Radiology (CT, MRI, PET) Software
- [ ] Bed Management Software

Telecommunications

- [ ] Voice-Over IP Phones
- [ ] Overhead Paging

Security Systems

- [ ] Door & Access Management
- [ ] Surveillance Cameras
- [ ] Weapons Detection Systems
- [ ] Mass Notification System

HR and Employee Access

- [ ] Employee Intranet
- [ ] People Management Software
- [ ] Payroll Access
- [ ] Patient & Employee Safety Reporting
- [ ] VPN Access

Revenue Cycle

- [ ] Third-Party Billing Applications
- [ ] Supply Chain Management Software

Regulatory Reporting

- [ ] Daily Hospital Reporting Access (e.g., the New York State Department of Health [DOH], Hospital Capacity Direct Access [HCDA], Health Electronic Response Data System [HERDS])
- [ ] Epidemiology Reporting (e.g., RedCap)
- [ ] Quality Reporting to DOH

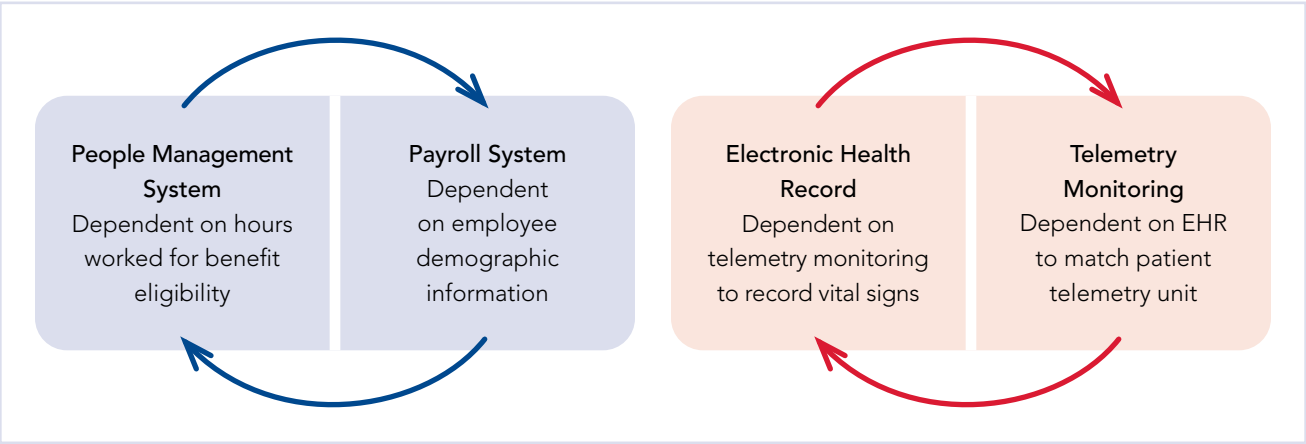
External Facing Systems

- [ ] Patient Portal (e.g., DOH HCDA, HERDS)
- [ ] Telehealth Services
- [ ] Website

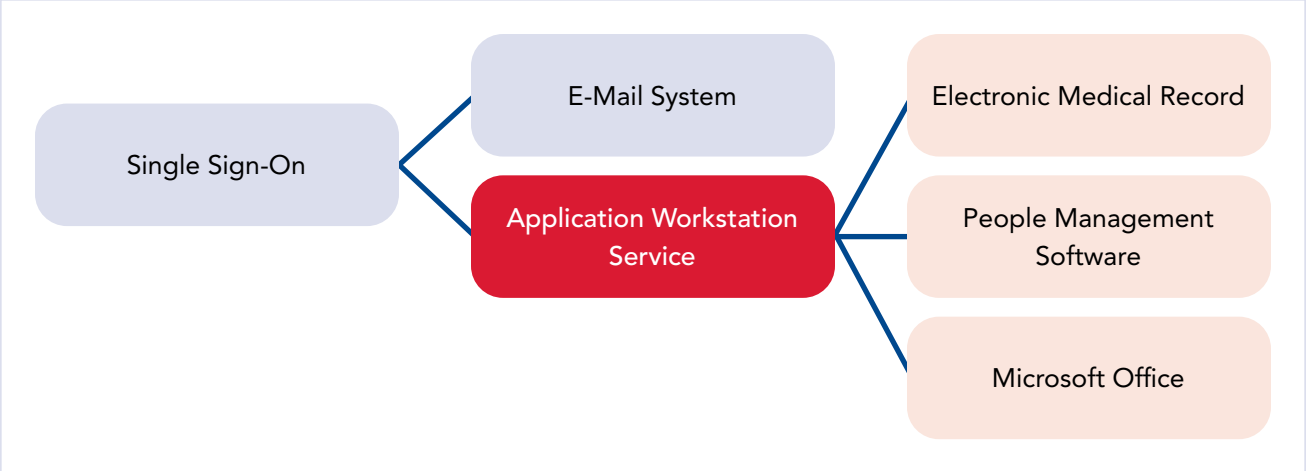
Scoping Affected Systems/Functions/Services

IT systems are sophisticated, integrated, and codependent on each other. While a disruption to a single system could be obvious and seemingly limited in scope, other systems may have a limited or restricted ability to perform their function.

Below are two examples of co-dependencies in corporate and clinical environments.



More critical disruptions can have cascading effects on other systems. In the example below, employees use a "single sign-on" to access hospital IT applications. In this situation, a clinician working on a patient floor requires an application workstation service to access the critical software needed for patient care. While the EHR could be functioning, the application workstation service that allows the employee to use the EHR on that computer prohibits them from accessing it, plus several other needed applications.



Disruptions such as the example above may have workarounds to enable continued access to non-affected applications. Hospital operations, corporate services, and emergency management leadership must engage with your IT department's disaster recovery team to understand available workarounds and downtime procedures.

Leadership: Cyber Policy Group

Once the cyber disruption incident response team has determined that there are ongoing and escalating impacts to hospital operations, the cyber policy group (see page 8) should be engaged. This group should understand the full scope of the event and its impacts on the hospital and get high-level situational awareness. The conversation should include the following individuals:

Title	Name and Contact Information
Chief Executive Officer	Name: _____ Primary Phone Number: _____ Secondary Phone Number: _____ E-mail: _____
Chief Financial Officer	Name: _____ Primary Phone Number: _____ Secondary Phone Number: _____ E-mail: _____
Chief Operations Officer	Name: _____ Primary Phone Number: _____ Secondary Phone Number: _____ E-mail: _____
Chief Medical Officer	Name: _____ Primary Phone Number: _____ Secondary Phone Number: _____ E-mail: _____
Chief Nursing Officer	Name: _____ Primary Phone Number: _____ Secondary Phone Number: _____ E-mail: _____
Chief Information Security Officer/ Chief Information Officer	Name: _____ Primary Phone Number: _____ Secondary Phone Number: _____ E-mail: _____

General Counsel	Name: _____ Primary Phone Number: _____ Secondary Phone Number: _____ E-mail: _____
Communications/ Public Relations Officer	Name: _____ Primary Phone Number: _____ Secondary Phone Number: _____ E-mail: _____

Questions for the group:

- What are the clinical and non-clinical impacts that have occurred?
- What are the overall effects on current operations?
- What is the status of our emergency department (ED)?
- Does this need to expand into a full-scale activation?
- Has the cyber disruption been contained or is it continuing to escalate?

Actions to Consider:

- "Lock down" or disconnect all systems, including both critical and non-critical assets
    - While this will have the largest impact on operations, it could be advantageous if the disruption has not been contained or identified by your IT team
- Limit external or remote access into systems such as VPN
- Reset all passwords if the situation dictates it
- Engage with your external cyber legal counsel and cyber insurance company*
- Communicate to staff and departments on downtime
- Activate hospital command center and incident command system

* Cyber insurance companies have experience with cyber attacks and can connect your organization to forensic resources and counsel about breach, regulatory issues, and ransomware payment. They should be contacted early in the response as they are a valuable resource from a regulatory and IT perspective.

Escalation of Response

Once the cyber disruption incident response team determines that hospital operations have been impacted, the cyber policy group should be activated. While the cyber disruption incident response team focuses on hospital operations and patient care, the cyber policy group concentrates on the strategic direction of the hospital during the cyber disruption. The cyber policy group should also determine the need for any further incident management escalation.

Full-Scale Activation

The cyber policy group should determine when impacts on hospital operations are significant, and when HICS should be activated.[31]

ADDITIONAL QUESTIONS FOR THE CYBER POLICY GROUP TO CONSIDER

- What support is needed now to maintain patient care?
- Should we divert ambulances? (see page 27)
- Should we cancel/postpone elective procedures?
- Is extra staffing needed to support certain areas of the organization?
- Do any regulatory reporting requirements need to be considered immediately?

Timeline for Conversation: Discussions about activating HICS should occur when the disruption is determined to be prolonged and more support is needed beyond what the cyber disruption team and the cyber policy group can handle.

Department Engagement with IT Services

IT staff will be in high demand during a cyber disruption as they work to characterize and resolve multiple technological issues. Leadership and department staff should ensure meaningful engagement with their IT department during this time, recognizing that outages have likely affected many, if not all, departments.

Questions and concerns about when certain technology will be back up and running should be triaged through department downtime leads and raised via your organization's HICS chain of command.

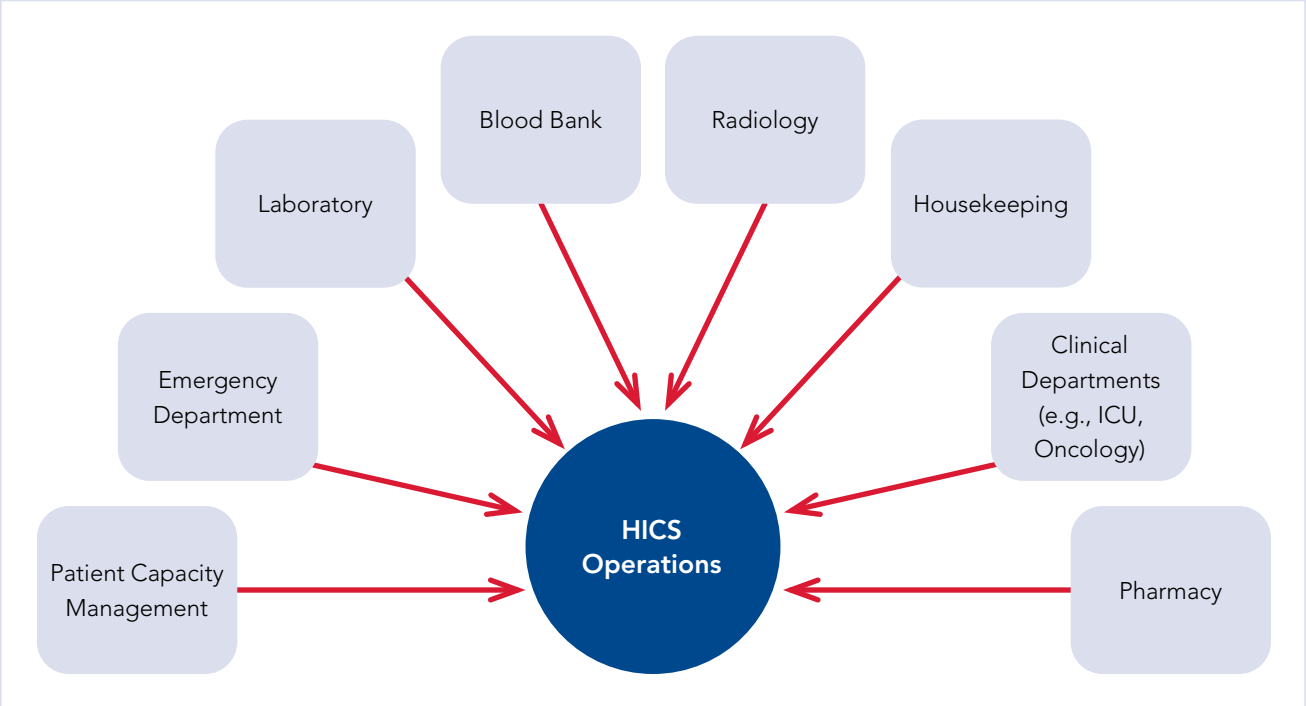
Department Command Centers

HICS provides overall support for general hospital operations throughout the course of a disruption. Individual departments may want to establish their own command centers to better support specific operations. Department downtime teams, where established, should lead these efforts.

During the early days of a disruption, departments must determine their most pressing needs and issues and seek to resolve them or develop workarounds.

Departments could also benefit from involving representatives from other areas in their operations. For example, housekeeping and patient capacity management are codependent and are both tasked with ensuring the timely turnover of bed cleaning and patient placement. These functions could also require a taskforce of representatives from multiple departments who work to ensure the continuity of a particular function.

Department command centers and any developed taskforces must be linked to the HICS structure to ensure decision-making and information are shared throughout the organization.



OPERATIONAL IMPACTS

Downtime Reduction of Patient Volume

While continuing patient care during downtime is most important, during a cyber disruption many systems could be offline. Maintaining patient care may therefore be difficult. To safely continue operations, your organization may have to determine ways to reduce patient volumes if staff is strained and procedures may have to be put on hold.

CASE STUDY

Burlington, Vermont – University of Vermont Medical Center[11]

The University of Vermont Medical Center's systems were offline for 25 days during their cyber incident. The oncology department set up multiple command centers that handled different functions to maintain patient care during the disruption.

- Outpatient Infusion Command Center
  - Centralized mechanism to gather data (paper charts and paper database)
  - Served as the coordinating body for patient treatment prioritization
  - Coordinated expanded operating hours to accommodate more patients. This also included the coordination of additional shifts, traveling nurses, and covering physicians.
  - Managed network referrals for patients who were referred to complete their treatment
- New Patient Command Center
  - All new patients were evaluated and screened by a team of nurse navigators and oncologists, depending on their cancer type
  - Patients were put into two groups → recently established patients or new referrals

Options to reduce patient volumes include:

- Canceling elective procedures
- Canceling appointments (both in-person and telehealth)
- Diverting ambulances*
- Canceling outpatient services, which could include:
  - Blood draws
  - Imaging
  - Cancer treatment
- Canceling blood drives/donations
- Discharging patients who no longer require hospital treatment to post-acute care settings

These recommendations can help organizations alleviate the stress on the system. Decisions should be made with executive, emergency management, clinical, and IT leadership. The recommendations could be implemented all at once or gradually, given the operational circumstances of the disruption. This is a key discussion point for leadership and should be considered with other operational plans.

* Not all ambulances may need to be diverted. Hospitals should determine the criteria for diversion prior to an attack occurring and coordinate with local emergency medical services about any diversion needs for your facility, particularly for high-acuity services (e.g., stroke diversion for inoperable CT scanners). These diversions may be time-limited as downtime procedures are implemented (e.g., in-person machine reading of CT scans allow stroke treatment).

If these recommendations are implemented, you should provide a rough timeline for when these services could be back up and running. The communications department should be heavily involved in this process to ensure that both staff and patients know when services will be back online.

Physical Security Considerations

During a cyber disruption, security measures should extend beyond the digital domain to include protecting the physical campus. Security leadership is still responsible for patient and staff safety during technology downtime. While security systems—including access control, surveillance, and weapons detection systems—are key to maintaining the security of the facility, they could fail during a cyber disruption.

Security teams must be ready to revert to analog processes, which could require increased security personnel.

Security and hospital leadership should consider the following key policy decisions:

- Should we restrict visitors entirely or just to specific areas of the facility during a prolonged disruption?
- Can we leverage non-security staff to provide awareness in places security staff could be limited?
- Would establishing one point of entry allow for safer operations?

Other Security Considerations

- Develop and share an alternate response plan for individuals with behavioral emergencies, including alert provisions if mass notification/paging systems are down (e.g., overhead pages)
- Extend shifts to allow for extra coverage without online surveillance systems
- Develop forms for visitor sign-in logs
    - Include space for the visitor's name, where the visitor is going, who they are visiting, and their contact information (phone number and e-mail address)
    - Ensure accurate information by requiring identification
- Create downtime mechanisms to verify visitation details, including:
    - Verify patient location (e.g., receiving a patient manifest)
    - Ensure visitor is permitted to visit patient (e.g., call patient floor)
    - Determine alternate mechanisms for Megan's Law registry lookups, including using open internet resources*
- Determine alternate weapon detection mechanisms, including hiring a third party security vendor to help with manual screening of visitors
- Develop a strategy for employee verification and access, including vendors, and consider an employee-only entrance
- Consult with facilities engineering staff and safety officers to determine procedures to secure areas

* Megan's Law registry lookups are a typical matter of course for many children's hospitals. Hospitals should determine alternate mechanisms only if the registry lookup is a standard practice at your facility.

REGISTRY: MEGAN'S LAW

Security systems may automatically check the Megan's Law registry, which is used to query registered sex offenders. Each state has an open web-based portal for manual searches during visitor screenings.

- New York: https://www.criminaljustice.ny.gov/SomsSUBDirectory/search_index.jsp
- New Jersey: https://www.nj.gov/njsp/sex-offender-registry/index.shtml
- Connecticut: https://uwc.211ct.org/sex-offender-registry-connecticut/
- Pennsylvania: https://www.meganslaw.psp.pa.gov/Home/TermsAndConditions
- Rhode Island: https://risp.ri.gov/safety-education/sex-offenders

Revoking a Terminated Employee's Credentials

Removing terminated employees from all your network-connected systems, including prohibiting building access via their ID badge, is a crucial cyber hygiene practice. These steps will prevent any unauthorized access to your facility (digitally and physically) before, during, and after a cyber disruption.

Building and Life Safety Systems

During a cyber disruption, building and life safety systems such as fire alarms, HVACs, fire sprinkler systems, and generators can fail. While they may be segmented from other systems, many of these systems are still connected to a hospital's network. Hospital facilities and engineering staff should determine any impacts to building and life safety functions and ensure they remain online and functional. If they are non-functional, these systems can have detrimental impacts on the continuity of patient care. For example, your facility's HVAC system could be controlled centrally and be non-functional, which could affect the ability to maintain temperature in key spaces, particularly operating and procedure rooms.

Staff should work to determine the need for any contingencies, such as instituting a fire watch for an offline system. Report any problems or associated impacts through your organization's HICS structure.

EMERGENCY NON-PATIENT SHELTERING DURING A CYBER DISRUPTION INCIDENT

Severe weather that produces extremely hot or cold temperatures can result in more non-patients taking shelter in your ED. During a cyber disruption incident, your facility may not be able to offer non-patient sheltering depending on the scope of the cyber disruption. Hospitals should communicate with local social services during cyber disruptions.

For example, during a Code Red or Code Blue activation in NYC, hospitals should contact the Department of Social Services to indicate whether their facility is able to shelter non-patients.

IMPLEMENTING DOWNTIME PROCEDURES

Hospital departments must shift quickly to downtime procedures during a cyber disruption. The highest priority for clinicians during downtime should be to maintain quality patient care and safety.

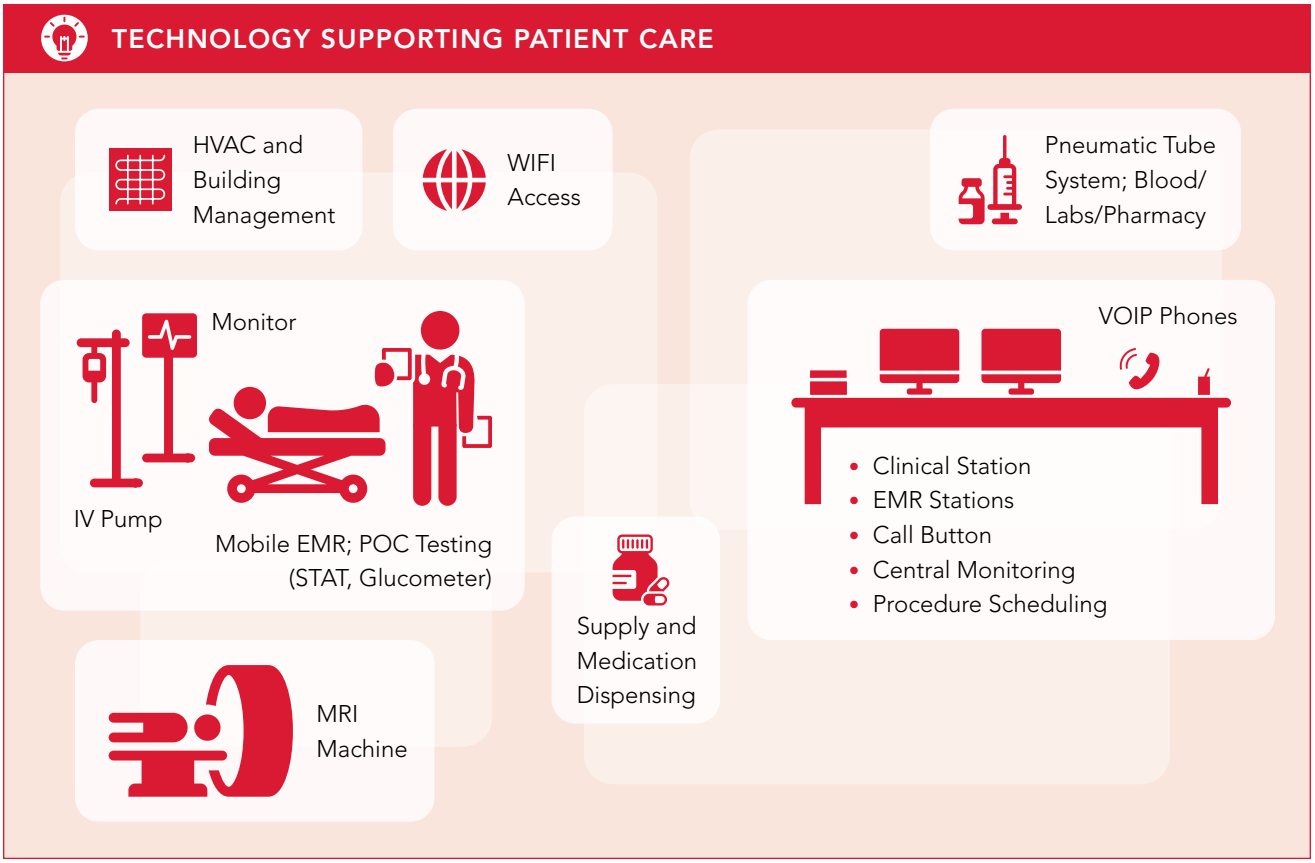
Leadership support is critical to staff who provide and support patient care and is a crucial aspect of a successful response. It also contributes to patient safety and staff morale. Communication, including updating staff about known timelines and shifts in operational policy, is key (see page 40).

Downtime procedures to consider fall into two categories: clinical and corporate services. Clinical refers to functions related to direct patient care and clinical support services such as pharmacy, laboratory, and radiology. The corporate services section further details functions such as payroll, revenue cycle, human resources (HR), and supply chain.

Clinical Downtime

Direct Patient Care Downtime

Technology directly supports patient care, enabling services or systems such as central and remote telemetry, heart monitors, or infusion pumps. Relying on technology can be detrimental to patient care during a cyber disruption.



Downtime Checklist: Patient Care Unit Operations

- [ ] Identify and retrieve downtime forms
- [ ] Follow typical procedures for downtime, as if it were routine downtime
- [ ] Identify and access your downtime computer, printing daily schedules and other pertinent details about current patients on the floor
- [ ] Conduct and document the patient census, confirming the status of all patients in the unit
- [ ] Conduct brief patient assessments on all patients, and if changes in clinical operations or care are expected, share them with patients and their family
- [ ] Establish paper charts. Make sure that all documentation has a detailed patient label on it.
- [ ] Document all clinical information (e.g., vital signs) on downtime forms, including patient demographics and identifiers

  Note: At least two points of verification are typically needed to ensure patient identity. Your organization's policies and procedures should highlight the exact patient identifiers needed.
- [ ] Conduct checks of all downtime supplies available in the unit and anticipate needs for additional shifts
- [ ] Determine discharge plans—including post-visit documentation and instructions, follow-up appointments, and prescriptions—working with social work services

The following general considerations and impacts can be anticipated when cyber disruptions impact patient care.

Impacts	Mitigation Strategy
Central/Remote Telemetry Monitoring	Place staff in high-risk rooms or cohort patients together to monitor them manually. Alternatively, transfer high-acuity patients to other facilities.
Registration Wait Times	Surge registration staff and consider opening alternate waiting rooms.
Medical Record Transfers	Ask IT or third-party suppliers about the deployment of additional copy machines.
Bed Placement and Monitoring	Develop alternate bed management worksheets using Excel or a cloud-based database. Ensure accurate hospital census periodically over the course of downtime.

SUPPORTING HEALTH EQUITY: DIRECT PATIENT CARE

Your organization's EHR details a patient's clinical information—medications, labs, and allergies, plus important information about who the patient is and how they identify. EHRs capture demographic information, including race, ethnicity, preferred language, age, and sex. In addition, many include sexual orientation and gender identity data, documenting the patient's gender identity, preferred pronouns, and preferred names. When a clinician is approaching the bedside, this information helps them to form an overall patient care plan. Your organization should consider how to obtain and maintain this patient information if the EHR can't be accessed.

Clinical Support Services Downtime

Clinical support services include services that provide diagnostic or ancillary support to patient care units. Implementing downtime procedures in these areas will ensure continuity and progression of patient care.

All clinical support services should conduct ongoing assessments of impacts to staff, space, supplies, and equipment. Unmet needs or identified issues should be shared with leadership or via HICS.

Clinical support services include a constellation of functions, including dietary, patient translation services, and social work, which are essential to delivering high-quality patient care. These departments should ensure that they have coverage during downtime for their services.

Additional function-specific considerations are provided below.

Laboratory Specimen Delivery and Results Reporting

- Laboratory staff should determine their testing capability given the scope of the incident. If certain tests cannot be performed due to downtime, clinical leadership should be notified through HICS.
    - Laboratory departments should engage with outside laboratory vendors to determine processes for offsite testing

- Clinical staff should use paper order forms with at least two patient identifiers to reduce incorrect test reporting. The more patient detail, the less chance for any reporting mix-ups.
    - Make sure there are several patient identifiers, plus all requested lab tests
    - Specimen collection vials should also contain sufficient patient identifiers. Order forms should be placed in a plastic bag with the specimen.
- "Runners" may be necessary if pneumatic tube systems are down. Labor pools (see page 35) can be leveraged to help deliver patient specimens.
    - Runners providing results to patient units should verify results through patient identifiers
- Laboratory staff should establish a quality control coordinator for any specimen brought for testing to:
    - Ensure all orders are properly documented before processing
    - "Stat" or urgent orders are prioritized over routine laboratory orders
    - *Note: While it might seem easier to file results based on the date of service, this could lead to more confusion since many patient units or patients themselves may not remember the date of service. To pull up patient results in a timely fashion, orders and results should be separated (inpatient vs. outpatient) and then alphabetized.*
- Critical value labs that may have been flagged in EHRs should be verbally reported to clinicians to ensure timely attention is provided for patient treatment
- Lab results should be documented in triplicate, with results being recorded in a laboratory department file and in a backup to the patient unit

PAPER SERIES: ANATOMY OF A CYBERATTACK

Paper series on laboratory services during downtime at University of Vermont Medical Center:

- Part 1: https://pubmed.ncbi.nlm.nih.gov/35188549/
- Part 2: https://pubmed.ncbi.nlm.nih.gov/35188951/
- Part 3: https://pubmed.ncbi.nlm.nih.gov/35188562/
- Part 4: https://pubmed.ncbi.nlm.nih.gov/35188946/

Pharmacy Medication Orders and Delivery

- Medication orders should be shifted to paper order forms if your facility's EHR is on downtime
- Medication orders should include type, dose, frequency, known drug allergies, medication list (for contraindications and interactions), and patient location
    - Clinical providers should verbally ensure any patient allergies to medications prior to ordering
    - Orders should also have patient identifiers to reduce medication errors
- Pharmacy should designate a quality control coordinator for all medication orders to ensure the five medication rights
    - "Stat" or urgent orders should be prioritized over routine medication orders
    - *Note: While it might seem easier to file results based on date of service, this can lead to more confusion since many patient units or patients themselves may not remember the date of service.*

To ease processing and pulling the patient's medication orders in a timely fashion, orders should be separated (inpatient vs. outpatient) and then alphabetized.

- Pharmacies should engage leadership and establish the feasibility of providing medication for both inpatient units and outpatient care, if applicable
- Paper-based order tracking or flowsheets should be used to ensure orders have been received, processed, and delivered to patient units
    - Runners providing results to patient units should verify them via patient identifiers and require signature upon receipt of medications
- High-acuity units such as EDs and ICUs could benefit from having an on-unit pharmacist for rapid consultation and dispensing

THE FIVE MEDICATION RIGHTS

1 the right patient	2 the right drug	3 the right time	4 the right dose	5 the right route

Blood Bank

- Use O-negative whole blood for emergent patient cases to eliminate the steps for blood typing and crossmatching delays
    - Consider availability of O-negative blood on critical units, including trauma resuscitation in the ED and surgical ICUs
- Ensure close coordination with laboratory departments to confirm blood typing and crossmatching results are accurate and verified through at least two patient identifiers
- Runners could be necessary if pneumatic tube systems are down. Labor pools (see page 35) can be leveraged to help deliver blood products.

Radiology Workflow

Radiology departments must understand the capability of each distinct type of equipment, including MRI, CAT, PET, and x-ray machines. Leadership should be notified immediately of any operational changes via the HICS structure. Radiology downtime could have direct effects on providing emergent care such as myocardial infarction intervention, stroke care, and trauma treatment, forcing hospitals to divert these services.

The Patient Archiving and Communication System for radiology could be unavailable during downtime, requiring manual interpretation of images.

- Determine what radiology services can be performed given the scope of the incident
    - Radiology departments may consider limiting orders to cases and scale according to capability
- Develop radiologist call schedules to ensure 24/7 coverage for reading in-person images
- Ensure all order forms are filled and include matching patient identifiers

Patient Access & Registration

- Ensure adequate staffing is available to manually capture patient demographic information
- Leverage labor pool (see below) resources to augment staffing
- Secure all paper documents that contain PHI in locked file cabinets or other access control
- Request patients seeking care at your facility provide pertinent health information, which could include insurance card(s), medication list, and any other medical records that can help clinicians develop and implement a care plan
    - Ask your communications department to help amplify this messaging

Discharging Patients to Skilled Nursing Facilities or Home

- Ensure open communication lines with skilled nursing facilities (SNFs) to streamline the process without an EHR
- Copy paper medical records and necessary patient information for transfer to SNF
- Discharge papers and guidance that could typically be accessed via the patient portal should be provided in paper format, which could include handwritten notes or instructions from the discharging provider
- Ensure discharging provider has access to paper prescription order forms if access to electronic prescribing system is disrupted
- Determine a centralized location to file and store paper records to ensure access during reconciliation and billing (see page 43)
- Outpatient Referral Consideration: Determine how to establish new patients seeking treatment at your facility who have been referred as part of discharge instructions (e.g., outpatient oncology department)

Corporate System Downtime

While patient safety is the first consideration during cyber disruptions, business operations could have an impact on the continuity of patient care. Hospitals will still need medical supplies, adequate staff to treat patients, and funding and cash flow to operate. These three core functions should be prioritized after clinical departments have moved to downtime and have stabilized.

Staffing Disruptions and Labor Pool

Cyber disruptions could curtail services or prohibit certain business operations. Leadership must determine the disposition of impacted staff, which could include reassigning them to areas or units that need support, or in a worst-case scenario, furloughing staff.

Organizations should establish a central labor pool to help streamline the repurposing of employees who cannot perform their normal duties due to a cyber disruption. HICS leadership should determine the need for a labor pool during prolonged downtime and ensure central points for coordination. For example, a CNO or nursing supervisor should oversee the nursing labor pool, and HR should manage the non-clinical staff labor pool.

Requests for staff from a labor pool should be made centrally, ensuring department leadership define specific roles for reassigned personnel.

SUPPORTING HEALTH EQUITY: LANGUAGE ASSISTANCE DURING DOWNTIME

Patients have a right to receive health care services in their preferred language. Language assistance is a core service and legal requirement for all hospitals. The rules and regulations that guide hospital language assistance include the Americans with Disabilities Act, Section 1557 regulations, and Section 405.7 Patients' Rights regulations in New York State. Language assistance includes the use of qualified interpreters—both onsite or through video-remote-interpreting—and a wide variety of other auxiliary aids and services that range in their reliance on network connectivity.

A cyber disruption can have major impacts on language assistance programs. Network-dependent systems such as phones, tablets, and computers could be impacted during a cyber disruption. Johnson Memorial Health in Indiana experienced a cyber disruption that took many of their systems offline, including their remote translation services. In one case, nurses used Google Translate to communicate with an Afghan refugee who arrived at the hospital to give birth.[34]

Being able to effectively communicate with patients is a key component of their care. The loss of these language assistance services has a major impact on patients, their caregivers, and the staff.

Hospitals should consider available alternatives when these services are disrupted. Available workarounds could include:

- Non-network auxiliary aides such as communication boards in your facility's top three languages
- Phones or tablets that are not connected to the hospital's main network that will only be used during downtime
- Accessing verified language assistance platforms using personal devices. Language access coordinators should consult their legal department before using this method as it involves PHI.
- Patient documents that have been translated into languages other than English that are typically provided in the patient portal or EHR should be available in a printed format and maintained in your facilities downtime box (see page 13)
- Determine which members of your hospital's existing staff are qualified bilingual interpreters. This could help reduce the strain at the beginning of downtime while contingencies are being stood up.

CASE STUDY

Franklin, Indiana – Johnson Memorial Health

Johnson Memorial experienced a cyber disruption that prevented its fetal monitoring system from sending notifications to central nursing stations.[34] The hospital deployed nursing staff to each labor and delivery room to ensure consistent monitoring, which increased demands on staff and required longer work hours for employees. Increased staffing should be a recognized need during clinical preparedness efforts (see page 11).

Payroll/Compensation

HR and payroll systems may not be operational or be proactively taken down, preventing employees from being paid. To ensure the continuity of employee payroll, consider the following:

- Engage with payroll system vendors (e.g., ADP, Paychex) and your financial institution to understand impacts on employee payment
- Use the last payroll distribution as the basis for future interim payment to employees
    - This will require reconciliation when systems are restored, including pro-rating time, modifying for employee increases in compensation, and adjusting for actual hours worked and overtime
- Proactively communicate payroll changes to the employee workforce
- Ensure mechanisms to capture worked employee time for hourly employees
    - Develop manual timesheets and central collection processes

Finance & Revenue Cycle Downtime

Initial considerations and steps your organization may take during a prolonged cyber disruption could include requests for payers to suspend:

- Pre-authorizations for procedures
- Concurrent and retrospective utilization review
- Referral requirements
- Timely claims filing requirements

Other relaxations could also be requested, including:

- Waiving contractual obligations to verify eligibility or other benefits
- Extending time to perform delegated credentialing
- Deferring documentation for hospitalization and procedures

Finance departments will also need to develop manual, paper-based billing mechanisms. Finance should leverage the labor pool with the manual process of this work or consider a third-party vendor to assist.

Hospitals could also consider engaging payers about receiving advance payments to ensure cash flow for core operating expenses during a disruption.

All costs during and related to cyber disruptions should be recorded for potential reimbursement. Finance departments may create cost centers or other systems to track these expenditures.

Supply Chain Management

Ensuring critical supplies—particularly those that are delivered just in time—during a cyber disruption is key to the continuity of patient care.

Your organization should immediately contact vendors and request supply lists for pending deliveries. Discuss any pending payments and future supply payments, explaining the current state of your systems.

Organizations should work with hospital operations to evaluate supply lists for future orders and manual orders in anticipation of continued operations. Expect that systems will be offline for a significant amount of time. Organizations that use third-party vendors to manage inventory and ordering should evaluate their contracts and engage with vendors on plans for continued operations.

COMMUNICATIONS DOWNTIME

While effective communication as an organization is key to successfully managing a cyber disruption, many communication systems are susceptible to interruption due to their dependency on network and/or internet connectivity. Maintaining and updating staff, patient, and visitor communications is imperative to maintain trust, situational awareness and, ultimately, patient care delivery.

Internal and External Communications

The table below outlines communication impacts you can anticipate during a cyber disruption. While this list is not exhaustive, it highlights a hospital's normal mode of communication and potential workarounds to implement. Some of the workarounds require pre-incident planning and may not be effective to deploy "just in time," particularly those that require intervention from your IT department (see page 25).

Communication Impacts*

Mode of Communication	During a Cyber Disruption	Potential Workarounds
E-mail	Internal e-mail systems may be proactively taken offline.	Create group chats through cloud-based apps (e.g., WhatsApp, Telegram) or via text messages within your department using personal cellphone numbers.† Mass notification tools—usually administered by emergency management, security, or telecommunications—are effective ways to share information via employee personal e-mails and cellphones.
VoIP Phones	VoIP requires network connectivity and may be proactively taken offline.	Use personal devices to conduct phone calls.† Use runners from a labor pool to convey information between departments.
Landline Phones	Current phone networks use a computer connection to function.	Install and use a non-network-reliant, limited emergency phone system with stations in key locations (e.g., charge nurse desk, lab)
Secure Messaging	EHRs or other hospital messaging platforms may not work during a network outage.	Maintain a contact list of personal phone numbers offline. Have an emergency text distribution platform.

* Adapted from University of Vermont Medical Center paper on oncology response to a cyber attack.[11]
† Use of personal devices must align with HIPAA guidelines and provisions to protect PHI.

Mode of Communication	During a Cyber Disruption	Potential Workarounds
Faxes	Modern fax machines are digital and often rely on internet or network connections.	Use analog fax machines and place them in critical areas throughout the hospital. Use runners from a labor pool to convey information between departments.
Wired and Wi-Fi	Networks may go completely offline or have no internet connectivity.	Use the guest wi-fi network if it remains available. Consider purchasing and deploying portable network routers with cellular connectivity.
Patient Portal	There could be limited or no access to the patient portal during a disruption. Communication with patients may be restricted through normal means (e.g., EHR chats).	Leverage downtime computers to retrieve demographic information for individual patient outreach. Use signage (posters, flyers) throughout your organization. Provide updates through community-based organizations and social media posts.

While consistent communication with staff is key, investigations into cyber attacks could preclude all information from being shared. Information about ongoing criminal investigations may require confidentiality. Cyber disruptions may cause an increase in phone call volume, particularly if typical modes of communication are down. Phone numbers established for specific services can help boost hospital communications and streamline patient requests. Department command centers should be used to set up communication mechanisms for specific services (see page 26).

Media and Public Relations Strategy

Communications departments should prepare scripted messages that are tailored to each cyber disruption. Hospital leadership, including the legal department, should approve messaging prior to publication.

Consider using the following means to communicate with staff, press, and the public during a cyber disruption:

- Internal e-mail distributions
- Inpatient food service notes
- Formal media statement
- External website
- Social media, including Facebook, X (formerly Twitter), and Instagram

CYBER INSURANCE

Consult your legal department about services your cyber insurance policy offers, including third-party communications firms that specialize in crisis and/or cyber incidents.

Sample Pre-Scripted Message Template

Communication Method	Message
Employee E-mail Distribution	The hospital is experiencing a potential cybersecurity threat that is impacting our IT systems. Systems may be experiencing complete outages or slow network connections. IT has identified the following affected systems: EHR, HR management software, etc. Users of these systems should immediately move to downtime procedures. IT is determining the extent of the systems affected but has no current time for restoration. The hospital is investigating the cause of this IT disruption and will continue to provide updates as more information becomes available. Please report any disruptions not listed on this e-mail to name/e-mail.
Patient Portal/ Medical Record	The hospital is currently experiencing a potential cybersecurity threat that is impacting our IT systems. This may interrupt access to your patient portal. We apologize for the inconvenience.
Food Service Note	The hospital is currently experiencing a potential cybersecurity threat that is impacting our IT systems. You may notice our staff using paper documents or reverting to back-up measures to ensure that proper care continues uninterrupted. We appreciate your patience during this time.
Media Statement	The hospital is experiencing a potential cybersecurity threat that is impacting our IT systems. The hospital was alerted to the disruption on date/time. We are working to understand the full impact and to restore systems as quickly as possible. The hospital remains fully open and our ability to provide patient care is unaffected. *If a cyberattack is suspected or confirmed:* The hospital is working with agencies (e.g., the Federal Bureau of Investigation [FBI]) to determine if this interruption is due to a cyberattack. The hospital is taking this threat seriously and cannot provide further information at this time.
Public Website *Consider using a landing page if website is unavailable.*	The hospital is currently experiencing a disruption to our IT systems. You may have limited access to our website and/or patient portal during this time. The hospital remains fully open and our ability to provide patient care is unaffected.
Facebook	The hospital is currently experiencing a disruption to our IT systems. You may have limited access to our website and/or patient portal during this time. The hospital remains fully open and our ability to provide patient care is unaffected.
X (Twitter) *Consider 240-character limit*	The hospital is currently experiencing a disruption to our IT systems. You may have limited access to our website and/or patient portal during this time. The hospital remains fully open and our ability to provide patient care is unaffected.

Consider writing pre-scripted messages for multiple scenarios, including the initial recognition of the cyber disruption, recognition of a cyber attack, prolonged IT system outages, and recovery and resolution of the event.

Staff communication should reinforce applicable hospital social media policies and emphasize rules on transmitting PHI.

Communications departments may also consider the following:

- Timestamp all communications to ensure audiences are getting the most current information
- Dedicate a staff member to monitor social media and other media outlets
- Share press inquiries with the incident command team to triage and ensure accurate responses
- Establish a secure staging area for an in-person media presence
- Coordinate messaging with your legal department to ensure information does not interfere with ongoing criminal investigations

EXTERNAL ORGANIZATION OUTREACH

Hospitals may be required to contact external organizations (see page 45) during a cyber disruption or provide operational status information to local response agencies.

It could also be beneficial to voluntarily consult the below organizations for response and recovery purposes.

Organization	

FBI	• Lead Federal agency that conducts cybersecurity investigations
	• Provides resources to support hospitals including:
	  ◦ Incident response teams to assist with forensic discovery
	  ◦ Decryption teams to assist with ransomware events
	  ◦ International law enforcement connections to assist with certain cybersecurity breeches

State Department of Health	• State agency that regulates hospitals and other health care facilities • May require notification of cyber disruptions • May relieve burdensome regulatory and reporting requirements until systems are restored
Emergency Medical Services & Emergency Management Agency	Hospitals should contact them to: • Provide situational awareness • Notify of curtailment of medical services and patient diversion
Neighboring Hospitals	Hospitals should contact them to: • Provide awareness if they curtail critical patient services (e.g., stroke, myocardial infarction, trauma).

Organization	
HIE	Hospitals should contact them to: • Notify of systems disconnection • Seek assistance with patient records if EHR is inaccessible.
GNYHA	• Assist with Federal, New York State, and local regulatory relief • Liaise and advise on communications with insurers about downtime payments.

Recovery

Cyber disruptions in hospitals can last from hours to months. Hospitals should expect recovery to be contingent on length of downtime and complications in IT platforms. All systems will not be restored instantaneously. Leadership and IT must catalog and triage which systems, service lines, and staff require access first.

The recovery process will range from months to years and will overlap with normal operations, doubling the potential burden on staff. Hospitals should continue to leverage labor pools (see page 35) to help reconcile documentation and should consider using a temporary staffing agency for clerical work or offloading documentation scanning to a third-party vendor.

CLINICAL SERVICES

Reintegrating manually recorded documentation back into the EHR should be prioritized so that providers can review a patient's course of care during the disruption. Priority should be given to high-acuity patients and those who have a prolonged length of stay.

Outpatient and Elective Surgical Considerations

- Determine if patients were shifted to other outpatient practices and follow up with them about continued treatment
- Reconcile missed patient appointments and elective surgical procedures and reschedule them as soon as possible—prolonged outages could require triage or patient prioritization

EHR Reconciliation

Length and scope of downtime will dictate the amount of paper documentation that must be reconciled. Hospitals should identify early who will be responsible for ensuring a paper reintegration process. Hospitals must determine how paper documentation should be attached to EHRs and consider the following:

- Which elements of paper documentation must be manually transcribed into the EHR (e.g., lab values reported in the test results section)?
- Will paper documents remain on paper and be stored in a filing system?
- Can paper documents be scanned and uploaded into a database or EHR for manual viewing (e.g., lab values scanned into EHR but not logged with other electronic documentation)?

CORPORATE SYSTEM RECOVERY

Corporate systems may take longer to be restored, as direct patient care services should be restored first.

Supply Chain Management

Suppliers should be notified when normal ordering and payment resume. If paper checks were issued, supply chain management should match orders received with payments rendered and backlog them into supply chain management systems.

Payroll/Compensation

Communication with employees about additional changes in capturing timesheets and receiving payments is paramount. If paychecks were based on an employee's last timesheet before the disruption, reconciliation on a case-by-case basis will be required. Hospital leadership will need to establish a policy to address overpayments or underpayments with staff. Employment counsel should be engaged to ensure compliance with any applicable labor laws.

Finance & Revenue Cycle

Insurance carriers will begin the reimbursements and claims reconciliation process as soon as possible, particularly if reimbursements were provided without preauthorization or full documentation of patient cases. If your hospital experienced a cyber disruption, external systems reconnection may take time, particularly if connected entities request third-party forensic IT verification. Consider whether this process should be performed with EHR document reconciliation or after this process is complete.

Expenses incurred from a cyber disruption should be captured for potential reimbursement by your cyber and/or business disruption insurance. Frequent communication should be sent to any budget owners in your organization.

Communications Recovery

Communication continues to have an important role during the recovery process. Your organization should consider how a cyber disruption will influence your reputation and patient trust. Patients, visitors, and their families should continue to receive updates about disruptions and reassurance about care delivery as systems come back online.

Communication methods used during your response should continue to be leveraged. Consider engaging with other organizations, including community-based organizations and patient/family advocacy groups. Work with your community affairs department to reinforce and restore trust in your organization.

External agency investigations may be ongoing, prohibiting specific information about the incident and its origins from being shared with the public. Despite this, messaging should focus on your hospital's operational status and ability to effectively treat patients. Your general counsel and leadership should continue to approve any internal or public messages.

Legal & Regulatory Resources

Cyber disruptions trigger many legal and reporting requirements. GNYHA has developed several resources to help hospitals navigate different aspects of the legal landscape during cyber disruptions.

GNYHA LEGAL AND REGULATORY RESOURCES

Hospital Guide to Cybersecurity Reporting and Resources
This document outlines agencies and contacts to report a cyberattack and includes specific cybersecurity resources.
https://www.gnyha.org/tool/hospital-guide-to-cybersecurity-reporting-and-resources/

Cyber Insurance: Questions to Ask Your Broker
This resource is intended for use before an incident occurs. Hospitals should ask brokers these questions when they are shopping for new insurance or looking to renew it.
https://www.gnyha.org/tool/cyber-insurance-questions-to-ask-your-broker/

Webinar: Primer on Cyber Insurance
This program details common cyber insurance provisions. How to avoid coverage disputes and gaps and leverage non-cyber insurance to obtain coverage for cyber incidents and attacks is also covered.
https://www.gnyha.org/event/primer-on-cyber-insurance/

Webinar: General Counsel as Cybersecurity Quarterback
This webinar is for hospital in-house legal counsel to better understand the theory and actual practice of managing a cyberattack.
https://www.gnyha.org/event/general-counsel-as-cybersecurity-quarterback-webinar-for-in-house-attorneys/

For additional assistance in this subject area, please contact GNYHA's Legal, Regulatory, and Professional Affairs staff.

HHS CYBER PERFORMANCE GOALS

HHS has developed national Cyber Performance Goals (CPGs) to help health care organizations prioritize implementation of high-impact cybersecurity practices.[35] Essential goals should be considered the foundation for

health care organizations. Enhanced goals are more advanced cybersecurity practices and should be implemented after an organization has established a baseline. While many of the CPGs are technical, this toolkit helps to address non-technical consequences of a cyber disruption.

APPLICABLE CYBER PERFORMANCE GOALS

Essential Goals → Basic Cybersecurity Training
Ensure organizational users learn and perform more secure behaviors (see page 14).

Essential Goals → Revoke Credentials for Departing Workforce Members, Including Employees, Contractors, Affiliates, and Volunteers
Prevent unauthorized access to organizational accounts or resources by former workforce members, including employees, contractors, affiliates, and volunteers by removing access promptly (see page 29).

Essential Goals → Basic Incident Planning and Preparedness
Ensure safe and effective organizational responses to, restoration of, and recovery from significant cybersecurity incidents (see page 7).

Enhanced Goals → Centralized Incident Planning and Preparedness
Ensure organizations consistently maintain, drill, and update cybersecurity incident response plans for relevant threat scenarios (see page 7).

Conclusion

Cyber disruptions continue to rise as major threats across industries, but health care remains the most vulnerable, yet lucrative target. While a cyber disruption can cause major damage, the way to prevent, respond to, and recover from one is not unlike other threats that hospitals and health care providers prepare for. A robust, multidisciplinary preparedness plan that cuts across all hospital departments and engages all staff from the C-suite to the frontline is critical to maintain patient care, limit operational interruptions and downtime, and protect PHI.

Hospitals' reliance on technology for almost every aspect of patient care increases their vulnerability to attacks. A cyber disruption that cripples a hospital's infrastructure may significantly hinder their ability to provide timely treatment to patients who require complex care.

Cyber readiness is constantly evolving, and hospital IT experts work tirelessly to protect complicated, multifaceted technological infrastructure and ward off daily attempts to compromise their systems.

A key lesson learned from hospitals that have experienced cyber disruptions and attacks is that incorporating a culture of good cyber hygiene practices and engaging all staff on preparedness is critical to minimizing disruptions and responding to a disruption quickly with little impact to patient care.

GNYHA hopes that our members find this toolkit valuable and use the resources to complement or build upon their own preparedness plans and activities.

END NOTES

1 National Institute of Standards and Technology. (n.d.). Retrieved from: https://csrc.nist.gov/glossary/.

2 US Department of Defense. (May 2023). Retrieved from: https://www.defense.gov/News/Releases/Release/Article/3408707/dod-transmits-2023-cyber-strategy/.

3 H. T. Neprash, McGlave, C.C., Cross, D.A., et.al. "Trends In Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016–2021." *JAMA Health Forum* vol. 3, no. 12 (December 2022); 1–11.

4 US Department of Health and Human Services. (September 2021). Retrieved from: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html.

5 Ponemon Institute. (2023). Retrieved from: https://www.proofpoint.com/us/cyber-insecurity-in-healthcare.

6 Verizon. (2019). Retrieved from: https://www.verizon.com/business/resources/reports/dbir/2019/healthcare/.

7 L. Wasserman, Wasserman, Y. "Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)." *Frontiers in Digital Health* vol. 4, (August 2022).

8 US Department of Health and Human Services. (April 2022). Retrieved from: https://www.hhs.gov/sites/default/files/insider-threats-in-healthcare.pdf.

9 American Hospital Association. (n.d.). Retrieved from: https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety.

10 Ponemon Institute, "The Impact of Ransomware on Patient Safety and the Value of Cybersecurity Benchmarking," *Censinet*, January 2023. https://www.censinet.com/impact-of-ransomware-on-patient-safety-and-value-of-cybersecurity-benchmarking (accessed March 14, 2024).

11 S. Ades, Herrera, D.A., Lahey, T., et. al. "Cancer Care in the Wake of a Cyberattack: How to Prepare and What to Expect." *JCO Oncology Practice* vol. 18, no. 1 (January 2022).

12 T. P. Hanna, King, D.W., Thibodeau, S. "Mortality due to cancer treatment delay: systematic review and meta-analysis." *BMJ* (October 2020).

13 Ralston, W. (2020, November 11). "The untold story of a cyberattack, a hospital and a dying woman." *Wired*. Retrieved from: https://www.wired.com/.

14 Collier, K. (2021, September 30). "Baby died because of ransomware attack on hospital, suit says." *NBC News*. Retrieved from: https://www.nbcnews.com.

15 *Teiranni Kidd v. Springhill Hospitals, INC.*, Circuit Court of Mobile County, Alabama. (June 2020). https://www.documentcloud.org/documents/21072978-kidd-amended-complaint.

16 C. Dameff, Tully, J., Chan, T.C., et. al. "Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US." *JAMA Network Open* vol. 6, no. 5 (May 2023).

17 Landi, H. (2022, July 27). "Healthcare data breach costs reach record high at $10M per attack: IBM Report." *Fierce Healthcare*. Retrieved from: https://www.fiercehealthcare.com/.

18 King, R. (2021, August 11). "May cyberattack cost Scripps nearly $113M in lost revenue, more costs." *Fierce Healthcare*. Retrieved from: https://www.fiercehealthcare.com/.

19 Collier, K. (2023, June 12). "An Illinois hospital is the first health care facility to link its closing to a ransomware attack." *NBC News*. Retrieved from: https://www.nbcnews.com.

20 Kim, J. (2019, September 17). "New Global Research Shows Poor Data Security Practices Have Serious Consequences for Businesses Worldwide." *Business Wire*. Retrieved from: https://www.businesswire.com/.

21 Rivas, A. (2022, December 29). "Scripps Health Could Owe You $ for the 2021 Ransomware Attack. Here's How to Claim Your Settlement Payment." *NBC San Diego*. Retrieved from: https://www.nbcsandiego.com/.

22 Joint Commission Resources. (n.d.). Retrieved from: https://www.jcrinc.com/what-we-offer/high-reliability/.

23 Massachusetts General Hospital Center for Disaster Medicine, "Hospital Preparedness for Unplanned Information Technology Downtime Events: A Toolkit for Planning and Response." *Mass General Hospital*, July 2018. https://www.massgeneral.org/assets/mgh/pdf/emergency-medicine/downtime-toolkit.pdf (accessed June 1, 2023).

24 Administration for Strategic Preparedness and Response, "Healthcare System Cybersecurity: Readiness & Response Considerations." *ASPR TRACIE*, October 2022. https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf (accessed June 1, 2023).

25 New York eHealth Collaborative. (n.d.). Retrieved from: https://www.nyehealth.org/shin-ny/what-is-the-shin-ny/.

26 The Office of the National Coordinator for Health Information Technology. (n.d.). Retrieved from: https://www.healthit.gov/topic/standards-technology/consolidated-cda-overview.

27 Agency for Healthcare Research and Quality. (2023). Retrieved from: https://www.ahrq.gov/cpi/about/otherwebsites/clinical-decision-support/index.html.

28 Centers for Disease Control and Prevention. (2022). Retrieved from: https://www.cdc.gov/opioids/healthcare-admins/ehr/clinical-decision-support.html.

29 S. Phansalkar, Desai, A.A., Bell, D., et. al. "High-priority drug-drug interactions for use in electronic health records." *Journal of the American Medical Informatics Association* vol.19, no. 5 (September 2012); 735-743.

30 Julie A. Garrison, "UpToDate," *Journal of the Medical Library Association* 91, no. 1 (January 2003): 97.

31 A. D. Kaye, Cornett, E.M., Kallurkar, A., et. al. "Framework for creating an incident command center during crises." Best practice & research. *Clinical anesthesiology* vol. 35, no. 3 (November 2020); 377-388.

32 PricewaterhouseCoopers, "Conti cyber attack on the HSE: Independent Post Incident Review." *PricewaterhouseCoopers (PwC)*, December 2021. https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf (accessed June 30, 2023).

33 Campbell County Health (2019, September 20). "Service Disruptions at CCH; no ETA." *Campbell County Health Wyoming*. Retrieved from: https://www.cchwyo.org/.

34 Yousry, F. (2023, May 8). "Cyberattacks on health care are increasing. Inside one hospital's fight to recover." *NPR*. Retrieved from: https://www.npr.org.

35 US Department of Health and Human Services. (2024). Retrieved from: https://hphcyber.hhs.gov/performance-goals.html.

555 West 57th Street, 15th Floor, New York, New York 10019
p (212) 246-7100 | f (212) 262-6350
www.gnyha.org