Sentinel Event Alert

A complimentary publication of The Joint Commission

Issue 67, Aug. 15, 2023

Preserving patient safety after a cyberattack

Early one morning, staff at Princeton Community Hospital in West Virginia arrived at work to find ransomware notices on their computers. The hospital had been attacked by the Petya ransomware – a strain of ransomware that encrypts certain files on a computer then demands a ransom payment in exchange for a decryption key. Information on the hospital's electronic health record (EHR) was inaccessible to the hospital's staff, IT systems were unable to retrieve updates, and email was down.[1]

With many of the hospital's existing care systems inaccessible, this type of attack could have been disastrous for staff and for patients. Cyberattacks cause a variety of care disruptions which can lead to patient harm and have severe financial repercussions. Princeton Community Hospital knew exactly what to do.

Within an hour after the attack, the hospital implemented its incident response plan and began using paper and pen to order medications and lab tests. After evaluating the risks to patients, the hospital determined it could remain open, but emergency cases were diverted elsewhere. Surgeries and diagnostics were performed as usual, except for a few patients for which the hospital could not access allergy information.[1]

Using the hospital's cloud backup system and disaster recovery software, the hospital's IT team began running computers again 36 hours after the attack. Having a cyber insurance policy gave them access to experts and companies who provided assistance. While the incident was time-consuming and labor-intensive, its biggest impact was forcing the hospital to replace its hard drives and to patiently work to get all of its systems and related information back online.[1]

It could have been much worse if the hospital didn't have the plans in place to deliver care safely after a cyberattack. Similar cyberattacks have disrupted care and compromised patient safety at hospitals across the nation.[2,3]

It's critical that healthcare organizations do all they can to prevent a cyberattack, such as decreasing access points for penetration, removing devices with old or obsolete operating systems, and training and testing staff to decrease vulnerability to phishing. There is abundant guidance for healthcare and IT professionals on how to prevent cyberattacks; therefore, this *Sentinel Event Alert* focuses on the safety risks associated with such events and provides tips on what organizations can do to prepare to deliver safe patient care in the event of a cyberattack.

Cyberattacks in healthcare have grown steadily

The number of cyberattacks and information system breaches in healthcare has grown steadily, escalating from isolated incidents to widespread targeted and malicious attacks.[4] Moreover, the number of attacks is likely to be greatly underestimated because there is still a reluctance to report them. Department of Health and Human Services (DHHS) data revealed that 707 data breeches occurred in 2022, exposing more than 51.9 million patient records. The most common locations for breaches were network servers and email, with the majority involving hacking or other IT incident. Malicious cyberattacks have occurred in small, independent practices as well as in large, integrated and well-protected healthcare systems.[2] Because of this, indemnity insurance is now hard to get and often prohibitively expensive.

Published for Joint Commission accredited organizations and interested health care professionals, *Sentinel Event Alert* identifies specific types of sentinel and adverse events and high-risk conditions, describes their common underlying causes, and recommends steps to reduce risk and prevent future occurrences.

Accredited organizations should consider information in a *Sentinel Event Alert* when designing or redesigning processes and consider implementing relevant suggestions contained in the alert or reasonable alternatives.

Please route this issue to appropriate staff within your organization. *Sentinel Event Alert* may be reproduced if credited to The Joint Commission. To receive by email, or to view past issues, visit www.jointcommission.org.

Hospitals have tremendously increased their use of network and Internet-connected technologies, cloud providers, remote third parties and non-clinical workers, increasing the digital attack surface for cyber adversaries, said John Riggi, national advisor for cybersecurity and risk for the American Hospital Association. In addition, he explained that hospitals have in effect become data aggregators. They not only have large volumes of protected health information, they also have personally identifiable data on patients, including payment information. Many hospitals and health systems also have highly valuable medical research. All these data sets, individually and in combination, make hospitals a target-rich environment for cybergangs and nation state actors alike.

A survey of 641 healthcare IT and security professionals by the Ponemon Institute found that 89% of the respondents' organizations experienced cyberattacks during the previous 12 months. The most common kinds of attacks were cloud compromise (54% of respondents), business email compromise (51%), supply chain disruptions (50%), and ransomware (41%), with all of these attacks disrupting patient care.[3]

Over the last 10 years, 99 cyberattack, ransomware or hacking-related events were reported to The Joint Commission, 90% of which impacted hospitals. Some of these events were associated with harm to patients (e.g., delays in care).

All staff – not only IT – must be prepared

Preparing for a cyberattack should not be a concern for the hospital IT staff alone; all hospital staff must be prepared to operate during a cyber emergency. For most hospitals, experiencing a cyberattack that adversely affects operations is not an "if" but a "when" question. Hackers are very adept at finding new ways to intrude; therefore, it's difficult if not impossible for hospitals to rely solely on preventing attacks with cybersecurity.

Protecting networked systems considered to be life-critical or safety-critical areas are of particular importance. Virtually all data, devices, or workers connected via the Internet or hospital IT network create vulnerabilities for a hospital, including the electronic medical record (EMR) (including lab and medication orders), cloud providers, biomedical and medical devices (including smart devices), scheduling software, radiology and diagnostic technology, patient identification/barcoding, telehealth and telemetry, outside vendors, and remote workers. In addition, crucial support systems such as utilities, heating, ventilation and air conditioning, and refrigeration can be disrupted by an attack,[5] further compromising the organization's ability to deliver safe patient care.

Actions suggested by The Joint Commission

Joint Commission Emergency Management (EM) Standard EM.11.01.01 requires a hospital to conduct a hazards vulnerability analysis (HVA) that includes human-caused hazards such as cyberattacks. The identification of cyberattacks as a prioritized hazard would provide a starting point for hospitals to identify and implement mitigation and preparedness actions to reduce the disruption of services and functions and assure patient safety.

The Joint Commission also requires hospitals to have a continuity of operations plan (EM.13.01.01), disaster recovery plan (EM.14.01.01) and emergency management education and training program (EM.15.01.01) as part of a comprehensive emergency management program. Hospitals must annually evaluate their emergency management program, emergency operations plan, and continuity of operations plans. The following recommendations from the cited literature relate specifically to the cyberattack hazard.

1. **Evaluate HVA findings and prioritize** hospital services that must be kept operational and safe for an extended downtime. Organizations should be prepared to have life- and safety-critical technology offline for four weeks or longer.[6] These services include pharmacy (particularly medication order entry systems and medication reconciliation services); medical records; and laboratory, radiology and pathology, as well as other services required by a high volume of patients or patients of high acuity (for example, blood bank, critical care units, intensive care units, infant security, nutrition services, and oncology and transplant).[7,8]

The prioritizing process involves mapping the consequences of losing the support of the EMR and other technologies.[8] This process is particularly helpful toward identifying interdependencies and hidden dangers when systems can no longer connect to one another.[7,8]

Of significant importance are medication order entry systems that support dosage scrutiny, check for drug-drug interactions, alert about allergies, safely administer chemotherapy, and select proper weight-based dosing for pediatric patients. Ensuring access to medical history/results and making sure laboratory, radiology, and pathology can rapidly communicate test results to multiple clinicians also are high priorities.[8]

Other important, yet vulnerable, systems that must be kept safe relate to admissions, patient movement and transfer within the hospital, patient discharge, and referrals.[8]

Service outage may not be isolated to a facility. Preparation should anticipate disruption of service across a broad geographic area, especially if the Internet infrastructure is compromised. This will result in particularly acute challenges for hospitals that are running their EHR or other key systems as a "service" from a central installation. It also means that other hospitals or medical assets in the vicinity may be compromised, and contingency needs to be made for that circumstance.

2. Form a downtime planning committee to develop preparedness actions and mitigations, with representation from all stakeholders. Comprise the committee with IT experts, hospital operational leadership, and hospital emergency managers, as well as representatives from the admitting and scheduling offices, environment of care, human resources, inpatient units, medical staff, nursing, nutrition and food services, operating rooms and procedural areas, outpatient clinics, pathology and laboratories, patient and family advisory committees, patient safety, pharmacy, public relations/communications, risk management, and other areas as necessary. Including key outside vendors is also advisable, particularly if they will be needed during a downtime response.[8]

The committee's responsibilities can include reviewing and strengthening the organization's proactive IT risk assessment plan; developing and evaluating procedures and resources to be used during downtimes; advising leadership to be prepared for additional staffing or equipment requirements during downtimes; performing root cause analyses of safety, throughput, patient care consequences and communications after downtime events; and recommending training or other interventions to address safety concerns.[8] Leadership may decide to designate oversight of the downtime planning committee to the organization's emergency management committee, thereby facilitating coordination of the organization's hazard vulnerability analysis, downtime drills, and other activities.

Implementing downtime workflows to monitor high-alert medications

A patient with a history of a vascular condition was admitted with deep vein thrombosis during an EHR downtime. The patient was placed on IV blood thinners. When the patient was bridged to warfarin, there was no alert about a lipid-lowering medication the patient was taking that potentiated the effects of warfarin. In addition, lab work results took longer due to the downtime. The patient developed a gastrointestinal bleed. In this case, the loss of clinical decision support during an EHR downtime clearly had an adverse impact on the patient. As a result, the hospital's pharmacy implemented downtime workflows to closely monitor high-alert medications.[7]

Using outside resources to ensure continuity of care

After a cyberattack hit part of its network, University of Florida Health contacted pharmacies to retrieve missing medication information and sent patients to physicians outside of its network to ensure continuity of care. Ed Jimenez, CEO of one of the affected hospitals, recommends having emergency plans that integrate teams far beyond the IT department. "Legal, communications, procurement — we all need to partner on a shared playbook in case of an attack," he says. "Hospitals have an incident management process for active shooters, floods, and pandemics. Ransomware isn't any less special."[9]

Placing downtime code carts on each unit

A Boston-area hospital locates "Downtime Code Carts" on each unit. These one-stop-shops for all downtime resources required by the staff help to speed the transition to safer downtime care. Like other code carts, they can be equipped with break-away locks to clearly indicate when they have been used, and when they need resupply.[8]

3. Develop downtime plans, procedures and resources. To keep patients safe and to maintain hospital operations after a cyberattack, develop and regularly update plans and procedures to be followed during downtimes, including when to declare downtimes, shut down electronic systems, or limit or cancel elective procedures or services.[7] Ensure that these plans and procedures are

consistent with the organization's Emergency Operations Plan (EOP).[8]

"Downtime packages" can include having fax capabilities; paper and pen resources for ordering admissions, lab and radiology tests, medications, referrals and discharges emphasizing warm handoffs, food services, materials and supplies; as well as forms for coding and billing purposes. Store them offline in a central, visible location and have them readily at hand to quickly address key areas of vulnerability, along with medical and medication reference texts. For optimal results, create paper resources that match the format of your electronic systems and workflows rather than using older forms that were discontinued when electronic systems were established. Use personal devices to access web-based references and calculators during downtimes.[7,8]

- In the pharmacy, establish a pharmacy hotline and have enough fax machines to handle all orders, including a dedicated fax machine for STAT orders. Use runners to pick up medication orders and renewals and to deliver medications. Implement manual or double-check processes to avoid errors in the absence of barcode verification.[7]
- Maintain the capacity to perform critical tests in the lab, pathology and radiology and communicate results to providers. Achieving this goal requires having adequate staffing, ordering tests judiciously during downtimes, and developing working relationships with outside contractors to meet overflow demand.[7]
- Develop a protocol for how to inform patients using biomedical devices of any attack that may compromise devices.[10]
- Develop a method for scheduling, checking in, processing and documenting patient visits during a downtime. Collect all information necessary on a paper form to register a patient in the EHR after it goes back online, including medical and family history, allergies, medications, diagnoses and symptoms.[11]
- Identify alternative ways to print medical records, patient identification tags, follow-up instructions, educational materials, after-visit summaries and other life-critical and safety-critical information, and to develop charts that contain essential information for safe patient care.[7,11] Document how to transfer patients if necessary and how to attach medical records and patient IDs to them. Establish transfer agreements with other local hospitals to facilitate the transfer of patients for procedures that cannot be accomplished during the downtime.
- Provide instructions on how to engage with law enforcement, cyber-insurance companies, reporting and regulatory agencies, and cybersecurity vendors well in advance of an attack, including how and when to implement downtime protection and business continuance software.[8]

Organizations may choose to create redundant systems by maintaining offline, encrypted backups or critical data and investing in cloud or web-based solutions that provide alternative pathways to key information and processes, as well as in failsafe computer terminals that capture critical downtime clinical information on key units.[7,8,12]

Failure Mode and Effects Analysis (FMEA) is a proactive method that enables healthcare organizations to identify and mitigate risks. This approach enables organizations to correct issues identified during the process before an information system fails and to take steps to avoid a failure.[13]

4. Designate response teams. Form an interdisciplinary team to mobilize your organization in response to unanticipated downtime events. The team's responsibilities will include evaluating the severity of the cyberattack, deciding whether or not to take the organization into full downtime mode, directing staff to take the steps required to ensure patient safety, and communicating with organizational leadership. The Center for Disaster Medicine at Massachusetts General Hospital's (MGH) initial Downtime Assessment and Response Team (iDART) three-tiered process (see sidebar on next page) uses an initial team to assess the downtime event and its impact on the organization and another team to manage a severe situation.[14]

5. Train team leaders, teams, and all staff on how to operate during downtimes. Train team leaders and teams about the kinds of incidents that would cause a downtime to go into effect. With all staff across all shifts, include information about downtime carts and procedures in new employee orientation. (Staff includes all people who provide care, treatment, or services in the organization, including licensed practitioners; permanent, temporary, and part-time personnel; contract employees; volunteers; and health profession students.)[15]

Develop drills and exercises to give staff familiarity with downtime resources, including how to access and use paper resources and redundant systems.[7]

"The bottom line is you have to drill it often, so people are familiar with it. Whether it be a redundant system or a paper manual system, you have to practice it often," said Jim Kendig, the Joint Commission's field director, surveyor management and support, Division of Accreditation and Certification Operations. "Practice makes perfect, and perfect practice makes perfect. It's important to orient staff on what happens when electronic systems are unavailable." Drills can occur annually or quarterly, depending on various factors, including staff turnover and previous downtime experience.

Organizations also may want to develop a "clinical continuity" plan. Similar to a "business continuity" plan – typically an IT responsibility – a clinical continuity plan includes, for example, contingency plans on how to treat stroke, trauma and heart attack patients without the availability of normal imaging technology and catheterization labs, and how to continue delivering radiation oncology and chemotherapy.

A robust training program incorporates a variety of modalities including classroom training, workshops, tabletop exercises, and perhaps even a full-scale exercise to simulate a downtime event. Include cyberevents as a possibility in regional disaster plans. These trainings not only prepare staff but also serve to test procedures and resources and update them if necessary.[7,8]

Be prepared to provide healthcare support to staff who experience fatigue and other medical symptoms due to working extended shifts.[8]

6. Establish situational awareness with effective communication throughout the organization and with patients and families. Avoid delaying decisive action when a cyberattack occurs. Communicate which systems are impacted, as well as which ones are not.[7] Be clear about both clinical and non-clinical ramifications and about when downtime procedures begin.[11] Communicate what is being done to address the situation and provide frequent status updates. Communicate also with key clinical affiliates and off-site staff and providers, as well as with patients and families as necessary to assure that patient care is safe.[7,11]

To prepare in advance, pre-scripted templates and talking points for both internal and external audiences can help leverage communication tools more effectively during a response, especially with the initial notification of a downtime event to staff, patients and families, and other audiences.[8,16]

Mass General's iDART process

The Center for Disaster Medicine at Massachusetts General Hospital developed the iDART process that allows a small, multidisciplinary team (Tier One) to assess the severity of a cyberevent. This team then calls upon a dedicated multidisciplinary response team (Tier Two) to manage the incident if warranted. If the incident is having a major impact on hospital operations, the Tier One team activates the emergency operations plan (Tier Three).

The Tier One team determines the criteria to assess severity. The members of this team must collectively have a diverse knowledge base, with knowledge of both IT and operational issues. A list of the members might include the IT administrator on call, hospital administrator on call, nursing supervisor, emergency department charge nurse, emergency preparedness manager on call, admitting office, and informatics clinicians.[8]

The Tier Two team is comprised of all Tier One members, as well as other key service line leaders representing areas such as facilities management, labor and delivery, laboratory, materials management, nutrition and food services, operating room, outpatient services, pharmacy, radiology, research operations, and security.[8]

A Tier Three response calls for activation of the Hospital Incident Command System (or equivalent) to provide a comprehensive framework that supports a rapid, organizational-wide response to the incident.[8] The organization ensures that the HICS members have the necessary background and training.

Post all communications to your workforce on your organization's online portal if the Internet is unaffected by the downtime.[8] Establish frequent leadership rounding on affected units, as well as frequent huddles among unit staff.[7] Other commonly used internal communication methods include townhall meetings for staff, analog phones, portable radios, public address (PA) systems, Voice over Internet Protocol (VoIP) technology, e-news-letters, videocasts or forums, backup mobile communication devices or applications, and clinical low voltage phones. Communication platforms such as Microsoft Teams or WebEx also can be used longer term.[16] In addition, be prepared to use alternate communication methods such as signs and flipcharts, secure texting, and pagers.[7]

Communicate to patients and families on hospital units that a downtime has occurred and how it may impact the patient experience, particularly in regard

to test or procedure scheduling, test results, medication orders, food and nutrition services, discharge or transfer, patient education, and medical record documentation. Provide assurance that patient safety and care is the organization's first priority.

Communicate with patients whose medical devices may be compromised by an attack, according to pre-developed protocols. Have IT security professionals available to help answer any questions on the policy and governance associated with medical devices. Be ready to engage with vendors or manufacturers of medical devices to understand vulnerabilities, risks and appropriate protection and response measures.[10]

Proactively manage all media to communicate accurate information and counter misinformation.[7] Be aware of any information sharing constraints imposed by law enforcement or other authorities. Carefully evaluate which information you can share with media, elected officials, regulators, and the public to avoid legal or compliance issues. Do not speculate about the cause and effect of cyber incidents.[16]

7. After an attack, regroup, evaluate, and make necessary improvements. Take steps to recover and protect systems, such as enforcing organization-wide password resets after an attack, factory resetting, and replacing compromised hardware and software as necessary. Adapt systems to the new needs and requirements revealed by the attack.[17] Meet all external reporting requirements. Restore electronic systems deliberately to ensure that clinical information is current and accurate.[7,8] Establish a process and assign staff for transferring data into the EHR through scanning or manual entry after it has regained functionality.[11] Authenticate all transcribed orders. Prioritize and assign workflows to categories of medication orders.[7]

In conclusion, the recent increase in cyberattacks, especially ransomware attacks, on hospitals and health systems means that the potential to experience a cyberattack that adversely affects operations is not an "if" but a "when" question. There are actions that hospitals and other healthcare organizations can take to prepare to deliver safe patient care in the event of a cyberattack by using the Joint Commission's Emergency Management (EM) Standards as a framework and following the suggested actions in this *Sentinel Event Alert*.

Resources

- Best Practices for Communicating Cybersecurity Vulnerabilities to Patients, U.S. Food and Drug Administration
- Cybersecurity webpage, U.S. Food and Drug Administration
- "Cybersecurity for the Clinician" Video Training Series, Health Sector Coordinating Council (hosted on YouTube)
- Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group
- Healthcare System Cybersecurity: Readiness & Response Considerations, Administration for Strategic Preparedness and Response (ASPR) Technical Resources, Assistance Center, and Information Exchange (TRACIE)
- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, Healthcare and Public Health Sector Coordinating Council
- Health Information Technology, U.S. Department of Commerce, National Institute of Standards and Technology

References

1. Davis J. How Princeton Community Hospital survived the global Petya attack. *Healthcare IT News*, Aug. 2, 2017.
2. December 2022 Healthcare Data Breach Report, *The HIPAA Journal*, Jan. 16, 2023.
3. Ponemon Institute. Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care, 2022.
4. Upendra P. Selecting a Passive Network Monitoring Solution for Medical Device Cybersecurity Management. *Biomedical Instrumentation and Technology*, 2021 Nov 1;55(4):121-130.
5. Healthcare Information and Management Systems Society, Inc. (HIMSS). Cybersecurity in Healthcare, 2021.
6. Executives for Health Innovation. Privacy & Cybersecurity. Podcast: A Conversation with John Riggi on Cybersecurity Risks Facing Health Systems. Part One: Preparing Health Execs for the Inevitable Cyber Attack, Jan. 19, 2023.
7. Academic Medical Center Patient Safety Organization (AMC PSO). Patient Safety Guidance for Electronic Health Record Downtime, Nov. 27, 2017.
8. Massachusetts General Hospital Center for Disaster Medicine. Hospital Preparedness for Unplanned Information Technology Downtime Events: A Toolkit for Planning and Response, July 2018.
9. Weiner S. The growing threat of ransomware attacks on hospitals. Association of American Medical Colleges. *AAMCNews*, July 20, 2021.
10. U.S. Food and Drug Administration. FDA news release. FDA informs patients, providers and

manufacturers about potential cybersecurity vulnerabilities for connected medical devices and health care networks that use certain communication software, Oct. 1, 2019.
11. American Medical Association. Guidelines for developing EHR downtime procedures, 2017
12. U.S. Department of Health & Human Services. Office of Information Security and Health Sector Cybersecurity Coordinator Center. 2022 Healthcare Cybersecurity Year in Review, and a 2023 Look-Ahead. Feb. 9, 2023. TLP:CLEAR ID#202302091300.
13. Asllani A, Lari A and Lari N. Strengthening information technology security through the failure modes and effects analysis approach. *International Journal of Quality Innovation*, 2018;4,5.
14. Institute for Safe Medication Practices (ISMP). Emergency preparedness: Be ready for unanticipated EHR downtime. *ISMP Medication Safety Alert! Acute Care*. 2022;27(17):1-5.
15. Joint Commission Resources. 2023 Comprehensive Accreditation Manual for Hospitals.
16. Administration for Strategic Preparedness and Response (ASPR) Technical Resources, Assistance Center, and Information Exchange (TRACIE). Healthcare System Cybersecurity: Readiness and Response Considerations. Updated October 2022.
17. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018.
