INSTITUTE FOR HOMELAND SECURITY

Operational and Clinical Impacts of Cyber Breaches

Adam Lee

Brandy Ferguson

Ashley Simon

Operational and Clinical Impacts of Cyber Breaches

Adam Lee MBA, MS, CEM, Brandy Ferguson MD, MS &

Ashley Simon MSN, RN, CEN, NPD-BC, SCRN

Abstract

In today's evolving healthcare landscape, ensuring the safety and readiness of healthcare facilities, staff, patients, and visitors is vital. This article underscores the critical importance of addressing cybersecurity operational preparedness in the healthcare sector, which is the most frequently targeted critical infrastructure. We will explore why these cyber threats pose significant challenges to the healthcare sector by examining the unique complexities and risks involved. Following this, we will discuss the challenges associated with preparing for and responding to these incidents. The article will also delve into preparedness efforts that can be undertaken to effectively mitigate these risks. By examining case studies and identifying best practices, we will provide healthcare organizations with strategies to improve their resilience against cyber threats. Ultimately, this piece will offer practical steps for enhancing an organization's ability to mitigate, respond to, and recover from these critical incidents.

Operational and Clinical Impacts of Cyber Breaches

Overview

According to the World Economic Forum, in 2023, Cybercriminals top target was Critical Infrastructure (CI). Of the 16 CI sectors, healthcare was the most targeted for ransomware (Akshay, 2024). This analysis is designed for practitioners specifically in healthcare, nursing, providers, and/or higher education programs as it relates. The overall goal of this review is to provide a high-level analysis of the impacts of cyber breaches to healthcare organizations.

Once the overall impacts of cyber breaches have been established, we will examine the clinical (nursing & provider) impacts, and identify what education is provided to prepare healthcare workers to be successful to operate during downtime (downtime is a term used in healthcare to describe operations without technology for both planned and unplanned events/incidents). Additionally, this review provides actionable recommendations to healthcare organizations to maintain a baseline readiness for extended downtimes caused by cyber breaches.

This review recognizes the impacts, frequency, and relevance of cyber breaches across all healthcare care entities; hospitals, hospital systems, primary care, ambulatory care, outpatient services, long-term care, post-acute care, behavioral health, medical device and equipment, pharmaceuticals, health insurance and payers, laboratories and diagnostics services, but this analysis focuses mainly on hospitals and hospital systems. This article has even greater importance to Texas due to the amount of healthcare infrastructure in the state. According to the American Hospital Directory (2023) Texas has 407 hospitals, California has 364 hospitals, New York has 214 hospitals, Florida has 211 hospitals, and Pennsylvania has

182 hospitals (these numbers are non-federal, short-term, and acute care hospitals). In addition to the number of hospitals in Texas, Harris County specifically is home to the Texas Medical Center (TMC) which is the largest medical complex in the world, has the world's largest children's hospital, and the world's largest cancer center. The TMC has 9,200 total beds, is the 8th largest business district in the United States, performs over 180,000 surgeries a year, and has over 10 million patient encounters per year (Texas Medical Center, 2024).

Introduction

When reviewing the impacts of cyber breaches in context of operational impacts there are six overarching themes that should be understood: (1) Cost, (2) Duration and Frequency, (3) Unintended Consequences (4) Patient Safety, (5) Privacy, and (6) Interdependencies of hospitals on other critical infrastructures.

Cost

Two key perspectives should be considered when looking at the cost of cyber breaches, particularly ransomware (the most common type): (1) the cost of paying the ransom and (2) the operational losses incurred. One of the first widely documented cases of a hospital paying a ransom occurred in 2016, when Hollywood Presbyterian Medical Center paid approximately $17,000 USD in Bitcoin after their systems were compromised (Winston, 2016). This was followed by the Erie County Medical Center cyber breach in 2017 where they faced ransom demand of $44,000 USD but opted not to pay. By 2018, the costs of ransomware had risen again, as seen with Hancock Health, which paid the Bitcoin equivalent of around $55,000 USD (Brook, 2020). In 2024, the average ransom payout was just over one million dollars (Diaz, 2024).

When discussing the operating losses incurred due to a cyberattack many examples exist

that can be utilized to illustrate the clinical and business impacts. For example, Alder (2021) states that Scripps estimated losses were around $112.7 million. IBM (2024) found that on average it cost healthcare entities $9.77 million to recover from the cyber incident. These figures do not include recent events such as Crowdstrike or Change Healthcare breach which will likely top $2.3 billion dollars in losses as a healthcare industry (Bazzoli, 2024).

Duration & Frequency

According to the FBI healthcare was the most targeted industry for ransomware in 2023 (Tahir, 2024). Neprash, et., al. (2023) cohort study *"Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021"* provides evidence that overtime, healthcare has become a much larger target for cyber hackers. In this study the authors found that from January 2016 to December of 2021 annual ransomware attacks more than doubled, with increasing sophistication and occurrence in large healthcare systems. Neprash, et., al., findings were in line with that of The U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) who found that in the last five years there has been a 256% increase in hacking breaches and a 264% increase in ransomware specifically (HHS, 2024).

When looking at the duration of cyberattacks in healthcare it is important to first establish that in healthcare and other industries the term "downtime" refers to the inability to utilize technology such as the electronic health record, communication modalities (including medical equipment). In 2023 the average downtime from a cyber related incident was 18.7 days. This was an increase from 2022 which was 16 days and 2021 which was close to 7 days (Petrosyan, 2023).

Unintended Consequences

After reviewing cyberattacks on healthcare entities, several unintended consequences come to light. For the purposes of this review, we will focus on one key consequences: impacts on patient volume. McGlave et al. (2024) analyzed Medicare claims data using the Tracking Healthcare Ransomware Events and Traits (THREAT) database and conducted hospital, market, and admission-level analyses, comparing these findings to claims data from confirmed hospital cyberattacks. This evaluation revealed that initial volume reductions ranged from 16.7% to 25.4%, with recovery to pre-attack levels occurring within 2-3 weeks. Among hospital services, imaging experienced the largest impact, with a 44.1% reduction in services during the initial stages of the attack. Additionally, ambulance-arrived ER visits decreased by 26.2% (McGlave et al., 2024).

Dameff et al. (2023) took a different approach, examining two US urban academic hospitals during the four weeks before and after a ransomware attack. Their findings suggest that hospitals undergoing cyberattacks saw reductions in both patient volume and ambulance traffic. Nearby facilities in the same region experienced a range of impacts, including increased census, longer waiting times, higher rates of patients leaving without being seen, and adverse effects on accredited program metrics such as stroke, chest pain, trauma, and transplant metrics, (Dameff et al., 2023).

Patient Safety

Emergency Care Research Institute (ECRI), an independent nonprofit organization who aims to improve safety, quality, and cost-effectiveness of care and the Institute for Safe Medication Practices (ISMP) released their annual *Top 10 Patient Safety Concerns* which identifies the 10 most frequent and severe patient safety concerns. These patient safety concerns

made the list because a cross-disciplinary team of ECRI and ISMP medical experts reviewed evidence and evaluated topics based on; (1) how serious would the harm be to patients if this were to occur, (2) how likely is it for this to occur, (3) if this were to occur how many patients would it impact, (4) how difficult is the problem to recognize and/or rectify once it occurs, and (5) would the issue place pressure on the organization. The top 10 patient safety concerns of 2025 are:

1. Dismissing patient, family and caregiver concerns
2. Insufficient governance of artificial intelligence
3. Spread of medical misinformation
4. Cybersecurity breaches
5. Caring for veterans in non-military health settings
6. Substandard and falsified drugs
7. Diagnostic errors in cancers, vascular events and infections
8. Healthcare-associated infections in long-term care facilities
9. Inadequate coordination during patient discharge
10. Deteriorating working conditions in community pharmacies (ECRI, 2025)

Cybersecurity breaches coming in at number in at number 4 again underscores the seriousness of this issue, specifically around patient safety.

Supporting the ERSI and ISMP patient safety report is, McGlave et al. (2024) where researchers compared data from the five weeks before the cyberattack to the attack period and found a 20.7% relative increase in-hospital mortality. Further analysis of nearby facilities revealed an even greater relative increase of 36%. Examining two hospital systems—one with 11 hospitals and another with 22 hospitals—similar findings emerged. Notably, among admitted

Black patients, in-hospital mortality saw a relative increase from 61.8% to 73%.

Privacy

Another significant concern surrounding cyber breaches in healthcare aside from patient safety, is the exposure of sensitive protected health information (PHI). A breach of this data can lead to identity theft and fraudulent activities. Medical record contains a wealth of personal information, including names, addresses, dates of birth and death, admission and discharge details, email addresses, phone numbers, Social Security numbers, medical history, insurance and financial information, prescription details, and Medicaid numbers.

The true value of a medical record compared to individual pieces of personal data lies in its longevity. While a stolen credit card can be quickly reported and replaced, medical records are permanent, making it difficult to detect and mitigate identity theft. This is reflected in dark web markets, where a single medical record can sell for over $1,000, whereas a Social Security number typically sells for just $1–$3 (Trevino et al., 2024).

Data from the HIPAA Journal (2009-2025) revels a steady increase in healthcare data breaches from 2009 to 2024, with a leveling off between 2021 and 2024. The five largest breaches of PHI included:

1. Change Healthcare (2024): 190 million individuals affected
2. Anthem Inc. (2015): 78.8 million individuals affected
3. Welltok Inc. (2023): 14.78 million individuals affected
4. Kaiser Foundation Health Plan Inc. (2024): 13.4 million individuals affected
5. Optum360 LLC (2019): 11.5 million individuals affected (Alder, 2025)

Overall, the value of a medical health record provides additional clarity as to why hackers continue to target the healthcare sector. Not only is the medical record more valuable than other

pieces of individual information, but the information from the medical record can be utilized repeatedly whereas individual pieces of information such as a credit card typically can be used once before fraudulent activity is detected.

Interdependencies

This section does not aim to identify all interdependencies between healthcare and other critical infrastructure sectors. Instead, it focuses on the broader impacts on healthcare when essential services such as electricity, water, and supply chains are disrupted. Understanding these indirect effects in crucial in assessing the potential consequences if cybercriminals target these sectors.

When hospitals experience power outages and rely on backup generators, their operational capacity is often limited, affecting the community they serve. Backup generators are primarily designed to support essential life safety systems and critical medical equipment, not to maintain full hospital functionality. This limitation can lead to several operational challenges, including postponement of elective surgeries, delays inpatient admissions, medication storage concerns, limited elevator access, HVAC system limitations, reduced lighting, laboratory testing constrains for temperature sensitive equipment, and diagnostic equipment downtime (Unified Power, 2025)

Water loss in hospitals can severely disrupt essential operations, impacting patient care and safety. Critical activities such as hand hygiene, drinking water, food preparation, and medical procedures require a reliable water supply. Additionally, water is vital for sanitation processes like flushing toilets, bathing patients, sterilizing equipment, and cooling IT systems. Facility functions, including fire suppression and HVAC systems, also depend on water. The CDC emphasizes that healthcare capabilities can degrade by 67% to 99% within two hours of

water services loss (CDC, 2024)

Disruption to supply chain can occur for a wide variety of reasons ranging from natural disasters to public health emergencies and or a panic reaction from the public. Regardless of causes the disruption of the supply chain ultimately challenges clinical staffs' ability to provide patient care (to varying levels depending on what specifically is disrupted in the supply chain). Commons supply chain shortages that can be seen due to disruptions are with personal protective equipment for healthcare providers, medication, and durable medical equipment. All of which come with their own set of issues should a disruption occur. For example, shortage of medical equipment could lead to negative patient outcomes or patient safety concerns, and shortage in medications could lead to medication errors due to altering standard operating procedures (Shore, et., al., 2022).

Clinical Topic Discussion

This topic discussion will go into detail on specific impacts of cyber events as it relates to, nursing, and providers. Overall, each section will provide insights on challenges faced and outline why these challenges are seen during downtime.

Clinical (Nursing) Perspective

When cyber breeches occur, nurses have a primary role and responsibility to ensure patient safety is maintained, communication and continuity of care continues with minimal interruptions, along with protecting protected health information (PHI). However, Nurses lack proper education on prevention of cyber breeches and downtime operating procedures both in the academic setting and in the workforce (Kramerer and McDermott, 2020). Both Kramerer and McDermott (2020) and Paul et. al. (2021), discussed the need for curriculum revisions in higher education nursing programs to include cybersecurity and paper charting and manually processes

for ensuring patient safety and continuity of care are maintained. Many Nurses and other healthcare professional lack the formal training on downtime procedures and manual paper charting leading to confusion, increased stress and frustration and inefficiency during EHR outage and patient safety risks.

Additional challenges Nurses are impacted by during lack of access to Electronic Health Records (EHRs) outages include minimal patient data such as medication history, allergies and socioeconomical information that can increase the risk for errors or missed care opportunities. Disruption to patient identification processes can lead to misidentification of patients causing errors and delays in care. Nurses are the primary care managers and care givers for patients during hospitalizations so when EHRs are not working, nurses struggle with downtime or manual paper charting. Paper Charing is time consuming and prone to errors and has specific legal rules that many newer generational nurses may not know. Those nurses who began nursing before 2009-2013 and earlier would have been exposed to paper or manual charting as it was before EHRs were required by the American Recovery and Reinvestment Act of 2009 which then progressed to regulatory expectations by HHS and CMS (CMS.Gov, 2010).

Areas impacted during cyber events and what that means to a hospital. When electronic heath records (EHR) or other healthcare technologies become in operable for a sufficient time (greater than 4hrs) due to cybersecurity events or even power issues, patient safety is at risk. Patient safety risk can include delayed or inaccurate documentation which can lead to adverse drug reactions or medication errors, especially with lookalike sound alike medications and high-risk drugs. Tracking and trending of patient's labs, diagnostics, vital sign trends and even patient's locations can impact timely interventions or treatment plans for patients.

During prolonged EHR outages "normal" operating workflows and processes are

disrupted and impacted. EHRs automate and allow for enhanced and standardized efficiencies in patient care. EHR outages increase workloads on nurses and healthcare team members due to manual documentation, different workflows that are unfamiliar or uncommon. This in turn slows care delivery and increases the risk for errors. Communication breakdowns also occur during standard care, patient admissions, transfers and discharges resulting incomplete handoffs. Areas of healthcare that have a primary safety impact include medication management with errors due to lack of automated safety checks. Diagnostics such as radiology and lab results are significantly delayed and risk the chance of inaccuracies without digital tools. Surgical and Procedural care is impacted as many procedures are now managed using systems that require network connection or EHR data to provide patient care such as Cardiac Ablations, pacemaker placement, endovascular procedures (Cardiac/Neurology), anesthesia machines and robotic surgeries. Maternal and Fetal care is impacted with lack of electronic fetal monitoring, causing for nurses to manually perform fetal heart rate assessments which can lead to higher maternal mortality rates and stillborn. Emergency Care is also impacted as patient throughput slows down and Emergency rooms that are already full become very overwhelmed with patients that ambulances will reroute, and elective and emergent surgeries could cancel. This has legal and financial implications to a healthcare organization such as automated charges are not able to be completed, and staff also could be without pay and patient charts are legal records. Along with recovery of accurate documentation after downtime is challenging, risking data integrity. The biggest and most detrimental effect of Cyberattacks causing EHR outages is the increased mortality rates and extended hospital stays.

Education received prior to entering workforce. Nurses receive a college education before becoming Licensed Vocational Nurses or Registered Nurses. During their training in a collegiate

setting, nursing schools follow the American Association of Colleges of Nurses (AACN) Essentials Curricular and framework These essentials set the standard for core knowledge for nursing programs. The AACN has an essential competency regarding EHRs Information Management and Application of Patient Care Technology. This essential is important as the knowledge and skills in information management and patience care technology are critical in the delivery of quality patient care. This essential focus through AACN is on the utilization of EHRs and not so much on how to manage paper charting or manual processes such as medication administration record (MAR), checking and verification of orders and manually safety checks to name a few. This is limited due to the dominance and importance to know the utilization of EHR systems in the workforce to reduce the amount of training time nurses need to become independent after their education.

In 2012, the National Council of State Boards of Nursing (NCSBN) advised prelicensure nurses apply concepts of information technology use to nursing practice by including it as an element in the 2016 NCLEX test blueprint in the management of care category. This licensure testing category is to include security plans, safe use of equipment, and reporting of incidents, errors, or variances (NCSBN, 2015). However, the AACN or NCSBN learning objectives do not include a concept related to cybersecurity in relation to EHR, PHI, or nursing informatics (Paul et. Al., 2021). In addition, despite the need to integrate this content into nursing degree programs, the recognition of properly educating nurses on their role in cybersecurity has faltered (Paul et. al., 2021).

Paul et. al. (2021) has indicated that newer nurses, providers and healthcare team members lack the experience writing unformatted notes and need basic instructions such as using black ink when documenting on paper, drawing a single line through errors and initialing, avoid

joint Commission “never” abbreviations, and include date, time and signature on notes.

Education received when in the workforce. Once nurses and other healthcare professionals enter the workforce, primary onboarding education and training focuses towards ensuring new nurses and staff are competent to perform skills and task related to their daily role and responsibilities. Additionally, newly onboarded staff work to become proficient in the EHR that they will be using during daily operations. Many healthcare organizations do not have a built-in training curriculum for downtime charting and manually process for new hires or on an annual reoccurring basis. When reviewing case studies from healthcare organizations that have been through large scale and long term EHR outages there appears to be a common theme in their areas for improvement. This includes annual reoccurring training based on educational gaps on downtime charting and manual processes, downtime drills and toolkits to prepare nurses and healthcare team members for outages emphasizing manual workflows and alternative care processes.

Barriers to implement additional education for downtime charting and manual workflow education for EHR or network outages can include minimum to insufficient budgeted education hours for training, limited buy in from hospital and departmental leaders, a lack of processes, resources and tools to implement and education on for downtime procedures and reduced understanding of what business continuity looks like for departments and the organization.

Kramerer and McDermott, 2020, state that “education of students and nurses on the importance of cybersecurity and downtime charting and procedures is critical to maintaining a safe standard of care for patients and protecting their PHI”. Another outlet to ensure ongoing education and awareness for experienced practicing nurses may be achieved through regulatory requirements in hospital accreditations and suggestions of licensure renewal for continuing

education hours on cybersecurity preparedness and business continuity operations during EHR or network outages.

Clinical (Physician) Perspectives

With the introduction of the Electronic Medical Record (EMR), physicians have made the switch from paper to electronic methods for recordkeeping and ordering. Daily charting no longer involves taking pen to paper. Patient's histories are now entered via keyboard and electronic dictation. Laboratory and radiology orders are no longer checked items on a written form; x-rays, computerized tomography (CT) scans, and Complete Blood Cell (CBC) counts can now be ordered with a simple click. While the EMR may add an ease for everyday operations, downtime is inevitable and unavoidable. From a short system update to a cyberattack causing prolonged downtime, physician must not become dependent on EMR. They must continue to familiarize themselves with the charting methods used by their predecessors. As quoted by Paul et al (2021), 'hospital systems have become almost totally dependent on computers, the internet, and EMRs to function. This reliance on technology brings vulnerabilities (Paul, et. al., 2021).

Planned downtime is an expected occurrence that provides hospitals with necessary system updates and upgrades. Physicians, nurses, and staff are given timely notice that the EMR will not be available. These planned events are meant to minimally disrupt delivery of patient care. A physician may fill out a small amount of provider notes and orders, while waiting to resume normal operations. This usually is a minimal inconvenience to the physician and the medical unit.

However, physician workflow during an unplanned, prolonged downtime may change dramatically. Access to lab results and imaging studies are not accessible via EMR and must be obtained by other means. Whether it is calling the lab for results or finding a radiology

workstation to obtain reports, a physician's workflow can be slowed, and adjustments to new downtime workflows must be developed to provide continuous quality patient care.

Unplanned downtime is becoming more frequent with the increasing number of cybersecurity attacks. In a recent article by Brian Owens (2020), he explains that hospitals are a frequent target of cyberattacks because hospitals 'hold a great deal of valuable confidential data and the move to EMR has made the data more valuable' (Owens, 2020). Cyberattacks can result in a prolonged, unplanned downtime event, which can impact how physicians work and how they deliver patient care. In 2024, the Crowdstrike Incident occurred during an operating system security update, and resulted in surgical procedure cancellations, ambulance diversions, and patient care disruption at hospitals and clinics worldwide (Fox 2024).

Areas Impacted During Cyber Events and What that Means to Hospital. Whether under normal or downtime operations, it is imperative that physicians provide quality care to patients. According to the American Medical Association Code of Medical Ethics, physicians must ensure that the care patients receive if safe, effective, patient centered, timely, efficient, and equitable (American Medical Association, n.d.). The Electronic Medical Record has become an essential tool for physicians in the delivery of patient care. According to Fitzpatrick and Ellingsen (2013), EMR systems improve the accuracy of patient information, continuity of care, and clinical decision-making (Fitzpatrick & Ellingsen, 2013). Lack of an EMR could result in medication error, inadequate physician handoffs during shift change, delay in lab and imaging results, and postponed surgeries and procedures.

An attack on the EMR can be detrimental on hospital operations and physician performance. Loss of EMR across a hospital system could cause delays in access to patient histories and previous hospital treatment plans, which can further limit physician access to data.

These limitations could result in redundancies in lab work, procedures (e.g. echocardiograms, imaging), and medication administration. Patient care plans can also be affected by data obtained from radiological images. Computed tomography (CT) and Magnetic Resonance Imaging (MRI) are examples of common modalities used daily in the hospital. A cyber event could render these machines inoperable or result in transmission delay of radiographic images. Reeves (2024) stated that radiology is 'operationally dependent on resources connected through local and wide-area networks, and an attack's impact can be extensive' (Reeves, 2024). Disruption in the Picture Archive and Communication System (PACS) or imaging archive could result in delayed access to medical imaging data or inability of the radiologist to access imaging for interpretation. Furthermore, this delay could compromise timely interpretation of images, which could result in delay in care or administration of life-saving treatment. (Chen et. al., 2021).

Not only can cyber events affect the Electronic Medical Record but also impact hospital infrastructure. Hackers could access the EMR, hospital network, and medical devices. Pallardy (2023) describes in his article, "The Unique Cyber Vulnerabilities of medical Devices", that many medical devices lack security protocols built into other medical systems. Devices, such as intracardiac defibrillators, medication infusion pumps, and glucose meters are susceptible to attack. Telemetry monitoring of patients could be disrupted. Surgical equipment could also be deemed unusable during an event (Pallardy, 2023). In 2015, University of Washington researchers conducted a series of experiments that showed the possibility of hacking a teleoperated surgical robot (Langston, 2015). Access to medications and medical equipment for procedures kept in network-controlled cabinets are at risk for attack; moreover, limiting physician access to medications and supplies, which could delay patient care. Cyber events in hospitals may force hospital administration to divert patients to other hospitals for care, which

could result in critically ill patients being sent to a hospital in another neighborhood, city, county, or state. In 2024, a cyberattack on the Ascension Health System operating in 19 states forced of their 140 hospitals to divert ambulances to other hospital systems. (Hanna et. al., 2024)

Education Received Prior to Enter Workforce. The foundation of physician education and skills begin in medical school. Medical documentation begins in the classroom (pre-clinical) and later used during clinical rotations. According to the Association of American Medical Colleges (AAMC), documentation of clinical encounters is a core competency of medical students. (Amiel et al, 2022) During the preclinical years, students learn how to conduct patient interviews, perform physical examinations, develop differential diagnoses, and determine patient care plans. Students learn specific elements to include in a provider note. Some elements include History of Present Illness, Past Medical and Surgical History, Review of Systems, Physical Exam, and Medical Decision Making. (Lai 2021) These notes can be developed on standardized patients, which are used during pre-clinical medical student education. Medical students then hone these skills during their clinical years while precepting on the patient wards and practice their documentation in the Electronic Medical Record. Physicians-in-training (residents) and attending physicians provide guidance and feedback to medical students on their documentation skills. As an essential component of medical training, the AAMC stresses that medical students should be able to 'communicate effectively, both orally and in writing with patients, patients' families, and colleagues. (Hammond et. al., 2012) With the use of EMR becoming more commonplace across healthcare systems, medical students may have limited training on documentation requirement during scheduled or unscheduled downtime procedures. Students may lack experience in paper charting procedures at their institution (including note writing, handwriting prescriptions, or ordering or lab/imaging studies). They may receive training on downtime procedures during

designated training classes or hands-on during an actual event.

Education Received When in Workforce. Once medical students graduate and enter the workforce in their selected specialty (e.g. internal medicine, general surgery, etc.), they are known as physicians-in-training or resident physicians (or residents). Their work is essential to the function of academic medical institutions. This work includes documentation in the Electronic Medical Record. Onboarding at their medical facility typically comprises on dedicated training on that hospital's EMR. Residents learn basic EMR workflow, including how to document admission and discharge patient notes (also known as history and physical or H&P), how to order lab work and imaging studies, how to document procedures, how to complete discharge patient instructions and prescriptions, and how to order any follow-up patient appointments. These training sessions can be in-person or virtual. Physicians practice these skills using online test patients, and are oftentimes, tested on their proficiency at the end of the session. EMR help desks are often available to guide the physicians if an issue with the EMR occurs.

Upon graduation from residency or fellowship training, these providers are known as attending physicians or attendings. At most medical institutions (academic or community based), onboarding for attending physicians is essentially the same as for residents and fellows. EMR training occurs before the first physician shift begins. Compliance training, which typically occurs annually, can help serve as an EMR training refresher for physicians. Updates to EMR or changes to EMR workflow are communicated to providers regularly. While EMR training is a regular occurrence, downtime training for physicians may not occur with frequency. Training may be in real-time during an event, or physicians may be given downtime paper documentation forms without any explanation. These forms are usually filled out by hand and include provider notes (H&P), patient progress notes, discharge instructions, lab and radiology ordering, and

prescription pads for handwritten prescriptions. As stated earlier in the paper, Paul et al. (2021) mentioned that newer providers and healthcare workers lack the experience of paper documentation, including use of black ink, avoiding Joint Commission 'never' abbreviations, and including time stamps on notes (Bilger, et., al., 2021) Being on prolonged downtime can add to the daily stress of a physician's workload, especially during a cyber event. This could result in patient safety events, lack of proper documentation, delay in care, and physician burnout. Regular downtime process training for physicians can lessen the burden of an already stressful environment and ensure physician confidence when a downtime occurs. Jenkins et al. expressed similar concerns in their analysis on downtime training. According to Jenkins et al., 'without regular (downtime) training, manual processes can sometimes be forgotten, especially during the stress of an unexpected and elongated downtime' (Jenkins, & Rathore, n.d).

Way Forward (Recommendations)

When looking at what can be done from a non-technical perspective to address this growing concern three main recommendations come to light. First, hospitals and hospital systems need to lean in on their partnerships with local colleges and universities to underscore the importance of the "dying" competency. Second, each hospital and/or hospital system needs to conduct a comprehensive gap analysis of their operational/clinical cyber preparedness levels. Third, hospitals and healthcare systems need to start increasing training and drills of downtime procedures.

Recommendation 1: Education Partnerships. This analysis underscores that the essential skill of paper charting and operating during technology downtimes are competencies that are being lost for future nurses and providers as they are primarily being prepared to operate in a digital environment. Colleges and universities are focusing

on equipping students to meet immediate clinical challenges and succeed in standardized testing, often relegating downtime competencies to a lower priority. However, the reality is that many new nurses and providers will encounter technology downtimes in their practice, and having this skill and knowledge is critical to continuity of care and patient safety. To address this gap, hospitals and hospital systems should leverage existing partnerships with colleges and universities to develop innovative strategies that reintegrates the traditional art of paper charting into current education curriculum.

Recommendation 2: Specific Comprehensive Gap Analysis. In tandem with recommendation number one, on education & partnerships, every hospital and hospital system should conduct a comprehensive gap analysis specific to operating during extended downtimes. An example of a specific comprehensive gap analysis can be seen in Appendix 1, *101 Considerations: Healthcare Cyber Operational and Clinical Preparedness*. It is important to note that no assessment will be a one size fits all, and it will need to be tailors to specific organizations, but this appendix will serve as a starting point of conversation to get the process going. The purpose of conducting a specific gap analysis would be to identify what you do well, but also where can your organization grow in this space. Once completed it is recommended that you develop a work plan to address these gaps, but this cannot be done in a silo, as you will find that some of these items may not be feasible to fix, and others may align with current strategic plans and/or initiatives. Results should be shared with a multidisciplinary taskforce/working group comprised of operations leaders, your Chief Information Security Officer, leaders in your Information Technology (IT) space, and your clinical leaders.

Recommendation 3: Increased Training and Drill on Downtime Procedures. Using the gap analysis to bridge and target specific knowledge deficits for all clinicians, a structured education plan and training curriculum and/or drills will allow for repetitive exposure and knowledge growth during a controlled environment where the clinicians can understand, ask questions, and retain the specific information needed. The concept of relying on or solely incorporating just in time training for downtime procedures or paper charting mimics the approach of sink or swim. Sometimes the sink or swim method is an effective modality of training but for Downtime procedures and paper charting, these are a high risks skills and events and when you really consider what impacts downtime procedures and paper charting have on patient safety, satisfaction, cost, and litigations, it is important to ensure staff are learning, and not just going through the motions and hoping it is correct and sufficient. Healthcare systems should really consider supporting, prioritizing and maintaining accountability to structured education, training, and exercises for downtime procedures and paper charting.

At minimum healthcare organizations should have layers of training and preparedness for downtime procedures and paper charting. Some ideas to consider is a knowledge baseline, by providing everyone with general knowledge to downtime processes and procedures specific to their role, legality, regulatory and safety concerns and test their retention of the knowledge.

Then provide sample charting tools or toolkits, that staff can use as a reference during drills, trainings, and even real-world events. Have process maps and department level workflows available for referencing as well. Ensuring there is enough paper forms, pens, flip charts, chart dividers, etc. to be used during a real-world event and training to

ensure clinicians/staff are familiar with tools.

Then use training and drills to assess and analyze what can be improved on. Adult learners do best by doing so the more times it is drilled the more clinicians are likely to remember how to do processes and perform during a stressful, real-world event.

Closing

When analyzing the operation and clinical impacts of cyber disruptions, a concerning picture emerges. Cyberbreaches are no longer just an Information Technology (IT) concern but a patient safety concern. These events are one of the top patient safety threats, with evidence linking them to increased mortality rates among patients admitted at the time of attack. From an operational standpoint, cyber breaches result in financial losses ranging form millions to in some case billions of dollars. On average cyberbreaches for healthcare organizations last nearly three weeks, leading to numerous unintended consequences. Affected facilities see a decline in patient volume, while nearby hospitals experience an influx of EMS and patient admissions, placing additional strains on their resources. As hospitals become increasingly interdepended and reliant on digital networks, the ripple effects of cyberattacks grow more.

From both a nursing and physician perspective, cyberbreaches introduce numerous potentially life-threatening consequences. The ability to document patient care on paper, once a fundamental skill, has largely disappeared form educational training programs. New nurses and physicians are primarily trained to navigate EHRs efficiently, but they receive little to no instruction on how to operate in extended EHR downtimes. Many receive just-in-time training during an actual event, which can lead to added stress and higher workload. As a result, when cyberbreaches occur many providers are not as prepared to adapt to paper-based documentation and alternative workflows.

To start overcoming these challenges three recommendations were made with the first being hospitals and health systems needing to partner with educational institutions to reinforce the need for continual education on downtime. It may not be appropriate for entire courses to be dedicated to downtime charting, but rather incorporating aspects of it in every class. From there all healthcare entities should conduct a gap analysis, and can use Appendix 1, *101 Considerations: Healthcare Cyber Operational and Clinical Preparedness* as a starting point, to assess where your program and facility are at in terms of preparedness for these types of incidents. Lastly, facilities need to come up with creative, innovate ways in increase training and drills for staff so that when your facility experiences a cyberbreach it is not something that is completely overwhelming for staff, and your team has the knowledge, skills, and competencies to provide the highest quality uninterrupted care.

Appendix 1: 101 Considerations: Healthcare Cyber Operational and Clinical Preparedness

Healthcare Cyber Preparedness Assessment		
This checklist is designed as a starting point of conversation to identify any gaps in your care delivery site's operational preparedness for full downtimes caused by cyber incidents. Note that some questions may not be applicable to all care delivery sites and are dependent on your information technology infrastructure**.**		
Plans, Policies, and Procedures		
Do you have a downtime/cyber insurance policy?	Yes	No
Do you have a downtime/cyber operational policy?	Yes	No
Do you have a downtime/cyber procedure	Yes	No
Do you have a cyber incident response plan?	Yes	No
Do you have a cyber resilience plan?	Yes	No
Are cyber response activities included in your vendor vetting process?	Yes	No
Do you have a business continuity plan?	Yes	No
Have you conducted a business process analysis in the last 24 months?	Yes	No
Have you conducted a business impact analysis in the past 24 months?	Yes	No
Do you have a policy/procedure defining which surgeries can be performed on an extended downtime.	Yes	No
Do you have a plan for how outpatient services will continue to provide service during extended downtime?	Yes	No
Patient Records		
Do you have a plan on how you will provide patient records upon request during an extended downtime?	Yes	No
Patient Registration & Admission		
Do you have a manual process for registering patients if you are in a downtime?	Yes	No

Is there an established downtime process for verifying insurance eligibility if automated tools are unavailable?	Yes	No
Do front desk and admissions staff receive yearly training on downtime registration procedures?	Yes	No
Billing & Claims Processing		
Do you have a manual process for capturing charges?	Yes	No
Do you have a manual process for submitting insurance claims during an extended downtime?	Yes	No
Is there a plan for reconciling billing errors post downtime?	Yes	No
Medical Coding		
Do you have offline access to ICD-10 and CPT coding references for manual coding?	Yes	No
Do you have a plan for how coders will review and assign DRG, CPT, and HCPCS codes if EHR access is lost?	Yes	No
Accounts Receivable & Payment Processing		
Do you have a process for tracking outstanding balances and patient payments during an extended downtime?	Yes	No
Is there a manual process for accepting and posting patient payments during an extended downtime?	Yes	No
Denials and Appeals		
Is there a process for how denied claims will be tracked and resubmitted manually?	Yes	No
Training and Drills		
Have you conducted a tabletop exercise on downtime procedures and processes?	Yes	No
Have you conducted a downtime drill (functional or full-scale)?	Yes	No

Do you conduct regular downtime communications drills (radios, satellite phones, amateur radios, etc.)?	Yes	No
Does your organization regularly train staff on downtime procedures?	Yes	No
Emergency Communications		
Do you have a communications plan in place if standard methods fail (main hospital line, call centers, etc.)?	Yes	No
Do you have a backup emergency code alert system for activating hospital emergency codes?	Yes	No
Do your emergency “red” phones get tested regularly?	Yes	No
Do you have a plan for how you will maintain communications with EMS and other healthcare partners?	Yes	No
Have you discussed what information you will share on your external website during a cyberbreach?	Yes	No
Do you have a backup method for staff email if it is impacted during a downtime?	Yes	No
Do you have quick reference guides on the unit that provides guidance and contact numbers for staff for a downtime?	Yes	No
Hospital Operations & Logistics		
Can your site operate in a full downtime for 30 days?	Yes	No
Do you have a 30-day supply of critical downtime forms to sustain operations or a means to print downtime forms for an extended downtime?	Yes	No
Have you discussed how will you communicate with environmental services that a room will need to be cleaned?	Yes	No
Have you discussed how you will communicate dietary needs and or restrictions to food and nutrition?	Yes	No
Does your site have a plan for accessing critical documents when all systems are down (not downtime forms but other documents)?	Yes	No
Do you have a plan for using runners and identifying where they will come from?	Yes	No

Do you have a plan if the pneumatic tube system fails?	Yes	No
Security		
Do you have a plan to print and distribute badges for new hires during extended downtimes?	Yes	No
Do you have a plan if access control systems fail (badges, keycards, etc.)?	Yes	No
Do you have a process for issuing temporary badges for contractors, vendors, students?	Yes	No
Do you have a backup method for securing restricted areas of electronic locks fail?	Yes	No
Do you have a plan/procedure for handling aggressive patients or visitors during a downtime or when communications fails?	Yes	No
Have your security staff been trained on cyber threat and response protocols to downtimes?	Yes	No
Facilities & Engineering		
Do you have a manual process for monitoring and adjusting HVAC?	Yes	No
Do you have a manual override system for elevators?	Yes	No
Do you have a plan for how you will ensure temperature control in critical areas (operating rooms, pharmacies, data centers, etc.)?	Yes	No
Do you have a plan for how you will maintain fire alarm and suppression system functionality if electronic systems fail?	Yes	No
Do you have a paper-based tracking system for maintenance request during a downtime?	Yes	No
Human Resources		
Do you have a plan for how staffing will be coordinated and adjusted manually if scheduling software is down?	Yes	No
Do department managers maintain a printed copy of employee schedules or have means to access them during a downtime?	Yes	No
Do you have a plan for how remote and hybrid staff will be handled during an extended downtime or if	Yes	No

remote workers are unable to work due to system access?		
Do you have a plan for how the labor pool will function or a manual call-in system for requesting additional staff during a downtime?	Yes	No
Do you have a plan for how new hires will be onboarded and credentialed during a downtime?	Yes	No
Do you have a plan for how new hires licenses and certifications will be verified during an extended downtime?	Yes	No
Do you have a manual method for documenting employee injuries or reporting of workplace incidents?	Yes	No
Is there a plan to provide employee support services during an extended downtime?	Yes	No
Is there a backup process for handling legal and compliance related HR documentation?	Yes	No
Do you have a paper-based system for tracking employee disciplinary actions and HR investigations?	Yes	No
Payroll & Timekeeping		
Is there a plan in place for processing payroll manually if electronic payroll systems are unavailable?	Yes	No
Does your care delivery site have a plan on how they will garnish wages during an extended downtime?	Yes	No
Does your care delivery site have a plan on how time will be tracked for employees who worked (including shift differentials, hazard pay, overtime, etc.)?	Yes	No
Clinical & Nursing Preparedness		
Does your care delivery site provide annual education on downtime documentation to nursing?	Yes	No
Does your site have plans to establish or utilize specialized telemedicine options in the event of an extended downtime?	Yes	No
Does your site have a plan for tracking metrics for regulatory, accreditation, and variance during an extended downtime?	Yes	No
Does your care delivery site have examples of how to complete critical downtime forms for units/departments?	Yes	No

Does your care delivery site have directions to guide nurses on filling out downtime forms?	Yes	No
Does your care delivery sites have a process in place for delivering orders to lab and radiology and relaying results of labs and radiology?	Yes	No
Does your care delivery site have manual patient tracking boards located in all patient care areas?	Yes	No
Do you have a list of which clinical equipment requires network access and their downtime alternatives?	Yes	No
Do your clinic units have a plan in place should central monitoring be unavailable (cardiac monitoring/tele sitting/electronic fetal monitoring, etc.)?	Yes	No
Case Management		
Do you have a printed emergency contact list for staff, social workers, and insurance companies?	Yes	No
Is there a manual process for conducting utilization reviews and ensuring services are appropriately authorized during downtimes?	Yes	No
Are patient and family education materials available to print in extended downtimes?	Yes	No
Do you have a paper-based process for tracking referrals, transfers, and consultations during a downtime?	Yes	No
Do you have a temporary process for obtaining prior authorizations manually if the EHR access is unavailable?	Yes	No
Radiology		
Can you store images for 30 days across all radiological modalities if PACS is down (x-ray, ultrasound, CT, MRI, IR, etc.)?	Yes	No
Do you have a backup system for uploading images for radiologist review?	Yes	No
Is there a documentation process for radiology image interpretation and reports?	Yes	No
If your site uses remote radiologist, do you have an agreement for them to be on-site during an extended downtime?	Yes	No

Are your radiologists credentialed to provide support at other sites during an extended downtime? Are they able to provide on-site support?	Yes	No
Are your providers credentialed to interpret radiographic images when a radiologist is unavailable?	Yes	No
Lab		
Do you have manual processes for tracking specimen collection, processing, distributing results, and storage?	Yes	No
Do you have a process for prioritizing urgent and STAT test during an extended downtime?	Yes	No
Is there a backup plan for blook bank inventory without electronic tracking?	Yes	No
Do your lab analyzers function independently of the hospital network?	Yes	No
Do you have a list of which instruments require network access and their downtime alternatives?	Yes	No
Is there a downtime process to record and communicate critical values to clinicians?	Yes	No
Pharmacy		
Do you have a process to override medication dispensers if they go offline?	Yes	No
Do you have a process for distributing narcotics when automated systems are unavailable?	Yes	No
How will medication orders be received and processed if the electronic health record is down?	Yes	No
Do you have a backup system for tracking and ordering medication inventory manually?	Yes	No
Do you have a manual process for verifying and documenting medication administration?	Yes	No
Do you have a system to alter staff of drug allergies and interactions without the EHR?	Yes	No
Do you have paper-based prescription pads secured for use in case of system failure?	Yes	No
Have you identified alternative suppliers if your primary is impacted?	Yes	No
Recovery		

Do you have a plan for how you will reconcile (lab, pharmacy, etc.), and store all downtime documentation to ensure accurate patient records?	Yes	No
Do you have a plan for how all images will be merged with the patient record?	Yes	No

Note: This table intentionally does not discuss technical questions as the aim is operational preparedness not technical preparedness.

References

American Association of Colleges of Nursing. (2008)/ The Essentials of Baccalaureate Education for Professional Nursing Practice.

American Association of Colleges of Nursing. (2011). The Essentials of Master's in Nursing Education.

American Hospital Directory. (2023). Hospital statistics by state. American Hospital Directory. Retrieved March 5, 2025, from https://www.ahd.com/state_statistics.html

American Medical Association. Code of Medical Ethics-Quality. https://code-medical-ethics.ama-assn.org/ethics-opinions/quality#:~:text=While%20responsibility%20for%20quality%20of,values%20of%20the%20medical%20profession.

Amiel J, Ryan MS, Andriole DA, Whelan AJ. Core Entrustable Professional Activities for Entering Residency: Summary of the 10-School Pilot, 2014–2021. Association of American Medical Colleges; 2022. https://store.aamc.org/downloadable/download/sample/sample_id/581/

Akshay, J. (2024). *These are the biggest cybercrime targets, and other cybersecurity news to know this month*. World Economic Forum. https://www.weforum.org/agenda/2024/04/cybercrime-target-sectors-cybersecurity-news/

Alder, S. (2021, August). *Scripps Health ransomware attack cost increases to almost $113 million*. Scripps Health Ransomware Attack Cost Increases to Almost $113 Million. https://www.hipaajournal.com/scripps-health-ransomware-attack-cost-113-million/

Alder, S. (2025, January 20). Healthcare data breach statistics. HIPAA Journal.

Bazzoli, F. (2024, October 14). *Cyberattacks are undermining patient care and their trust*.

Health Data Management. https://www.healthdatamanagement.com/articles/cyberattacks-are-undermining-patient-c are-and-their-trust?id=135267

Brook, C. (2020, August 12). *Following ransomware attack Indiana Hospital pays $55K to unlock data*. Digital Guardian. https://www.digitalguardian.com/blog/following-ransomware-attack-indiana-hospital-pay s-55k-unlock data#:~:text=Hancock%20Regional%20Hospital%2C%20a%20facility,the%20costly%20ransom%3A%204%20BTC.

Centers for Disease Control and Prevention, & American Water Works Association. (2019). Emergency water supply planning guide for hospitals and healthcare facilities. U.S. Department of Health and Human Services.

Chen, PH., Bodak, R. & Gandhi, N.S. Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations. *J Digit Imaging* **34**, 731–740 (2021). https://doi.org/10.1007/s10278-021-00466-x

CMS.Gov (2010) Electronic Health Care Records at a Glance. https://www.cms.gov/newsroom/fact-sheets/electronic-health-records-glance

Dameff, C., Tully, J., Chan, T. C., Castillo, E. M., Savage, S., Maysent, P., Hemmen, T. M., Clay, B. J., & Longhurst, C. A. (2023). Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. *JAMA network open*, *6*(5), e2312270. https://doi.org/10.1001/jamanetworkopen.2023.12270

Diaz, N. (n.d.). *Average ransom payments rise for healthcare: 6 notes*. Becker's Hospital Review.https://www.beckershospitalreview.com/cybersecurity/ransom-payments-increase-for-hea lthcare-6

ECRI. (2025). Top 10 patient safety concerns 2025. ECRI Institute.

https://assets.ecri.org/PDF/Top10PatientSafetyConcerns_2025_final.pdf

Hanna, J, Murphy, T, and K Foody. (2024, May 10). A Cyberattack Forces a Big US Health System to Divert Ambulances and Take Record Offline. https://apnews.com/article/cyberattack-hospital-system-ambulances-diverted-ascension-728ab2a0e5afaf7c344e46a5ce5ca42c#

Hammoud, M. M., Dalrymple, J. L., Christner, J. G., Stewart, R. A., Fisher, J., Margo, K., Pangaro, L. N. (2012). Medical Student Documentation in Electronic Health Records: A Collaborative Statement From the Alliance for Clinical Education. Teaching and Learning in Medicine, 24(3), 257–266. https://doi.org/10.1080/10401334.2012.692284

Jenkins C. and Z. Rathore. Don't Wait Until Your System Goes Down to Make a Business Continuity Plan. https://healthlinkadvisors.com/perspectives/downtime-preparedness/#:~:text="Many%20physicians%20don't%20know%20how%20to%20hand,with%20manual%20processes."%203:%20Train%20team%20members.

Lai J. (2021, Jan 26). EMRA Medical Student Documentation. https://www.emra.org/be-involved/committees/education-committee/medical-student-documentation

Langston, J (2015, May 7). UW Researchers Hack a Teleoperated Surgical Robot to Reveal Security Flaws. https://www.washington.edu/news/2015/05/07/uw-researchers-hack-a-teleoperated-surgical-robot-to-reveal-security-flaws/

Fox, A. (2024, July 19) Worldwide IT Outage Disrupts Healthcare Delivery. Healthcare IT News. https://www.healthcareitnews.com/news/worldwide-it-disruption-disrupts-healthcare-delivery

Fitzpatrick G and Ellingsen G: A review of 25 years of CSCW research in healthcare: contributions, challenges and future agendas. Comput Support Coop Work. 22:609–665.

2013.

Kramerer, J., McDermott, D. (2020) Cybersecurity: Nurses on the frontline of prevention and education. *Journal of Nursing Regulation, 10(4).*

IBM. (2024). *Cost of A Data Breach*. Annual Report. https://www.ibm.com/downloads/cas/1KZ3XE9D

Petrosyan, A. (2023, November 7). *Ransomware attacks average downtime U.S. healthcare by days 2023*. Statista. https://www.statista.com/statistics/1422159/us-healthcare-ransomware-attacks-downtime- average-by-days/

McGlave, C. C., Neprash, H., & Nikpay, S. (2023). Hacked to pieces? The effects of ransomware attacks on hospitals and patients. *The Effects of Ransomware Attacks on Hospitals and Patients (October 4, 2023)*.

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. *JAMA health forum*, *3*(12), e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

Owens B. How hospitals can protect themselves from cyber attack. CMAJ. 2020 Jan 27;192(4):E101-E102. doi: 10.1503/cmaj.1095841. PMID: 31988158; PMCID: PMC6989022.

Pallardy, R (2023, Nov 14). The Unique Cyber Vulnerabilities of Medical Devices. https://www.informationweek.com/cyber-resilience/the-unique-cyber-vulnerabilities-of-medical-devices

Paul, C., Bilger, E., Kango, G., Reyes, J., Catalonotti, J. (2021) Residency Program Preparedness for Prolonged Downtime: Lessons Learned from a Cyberattack. *Journal of*

Graduate Medical Education. http://meridian.allenpress.com/jgme/article-pdf/13/5/626/3267175/i1949-8357-13-5-626

Rainer, M. (2024, March 13). *HHS office for Civil Rights Issues Letter and opens investigation of Change Healthcare cyberattack*. HHS Office for Civil Rights Issues Letter and Opens Investigation of Change Healthcare Cyberattack. https://www.hhs.gov/about/news/2024/03/13/hhs-office-civil-rights-issues-letter-opens-investigation-change-healthcare-cyberattack.html

Reeves, K (2024, March 5). Cyberattacks: Not a Matter of If, but When. https://appliedradiology.com/Articles/cyberattacks-not-a-matter-of-if-but-when

Shore, C., Brown, L., Hopp, W. J., & National Academies of Sciences, Engineering, and Medicine. (2022). Causes and consequences of medical product supply chain failures. In Building Resilience into the Nation's Medical Product Supply Chains. National Academies Press (US).

Tahir, D. (2024, September 17). *Cyberattacks plague health care. critics call the federal response "inadequate."* NPR. https://www.npr.org/sections/shots-health-news/2024/09/17/nx-s1-5111590/cyberattacks-

Texas Medical Center. (2024, January 25). *About Us*. Texas Medical Center. https://www.tmc.edu/about-tmc/

Trevino, A., Cutler, A., Guccione, D., (2024, January 11). Why do hackers want medical records? Keeper Security.

Unified Power. (2025, February 4). How to prevent power outages in hospitals. Unified Power.

Winston, R. (2016, February 18). *Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating*. Los Angeles Times. https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-2016 0217-story.html

INSTITUTE FOR HOMELAND SECURITY

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water / Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Lee, A., Ferguson, B., & Simon, A. (2025). Operational and Clinical Impacts of Cyber Breaches (Institute for Homeland Security Report No. 2025-1010). Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/TD8F5