Cyber Attacks on Interoperable Electronic Health Records:

A Clear and Present Danger

by Lancer Gates, DO

There is a balance between health information availability and health information security. Cyber attacks present a clear and present danger to this balance.

The Apocolypse is Upon Us

The healthcare industry is the perfect cyber-attack victim because it depends on technology for patient care and revenue cycles. Today, the healthcare industry has become the number one victim of cyber attacks. In 2022, there were 1,463 cyber attacks per week globally.

Lancer G. Gates, DO, FACOI, is President of the Missouri State Medical Association for 2023–2024. He is a Hospitalist from Kansas City, Missouri.

Once attacked, hospitals must either (1) pay a ransom to the cyber-attackers (incentivizing and perpetuating future attacks on more hospitals) or (2) go on downtime (the average downtime for hospitals in 2022 was 24 days with an average cost of $10 million). Either way, access and resources for medical services are both compromised.

The nightmare scenario is a simultaneous cyber-attack at two or more hospitals in close geographic proximity. This two-hit hypothetical would compromise access to care for patients with time-critical diagnoses such as trauma services, code strokes, and code STEMIs.

Downtime and the Rapture

In November of 2023, the Fred Hutchinson Cancer Center in Seattle, Washington, was the victim of a cyber-attack. When the Cancer Center refused to pay the ransom, the cyber criminals directly emailed the Cancer Center patients, offering to remove their personal health information from the dark web for $50. Patients who did not accept the $50 offer received a threat of swatting (the act of

reporting a false claim of a crime to law enforcement so that SWAT teams arrive uninvited at a person's home address).

On December 19, 2023, cyber criminals attacked Liberty Hospital (LH) in Missouri. The criminals faxed a ransom note to the hospital administration. LH immediately went on downtime, and the emergency department closed to trauma, code stroke, code STEMIs, direct admissions, and incoming transfers. Neighboring hospitals provided midwest hospitality for patients requiring transfer for services suddenly unavailable at LH. Akin to the rapture, more than 50% of patients were either discharged from LH or transferred to neighboring hospitals by the end of the first day of the attack.

When the Computers Failed, the People Prevailed

When a cyber-attack occurs, patient transfers and ambulance diversions inundate neighboring hospitals. Typically, employed physicians have privileges at a single hospital, restricting their ability to assist at neighboring hospitals. During cyber attacks, this results in underutilizing physicians at the hospital under cyber-attack and overutilizing physicians at neighboring hospitals. To accommodate the increased patient volume at nearby North Kansas City Hospital (NKCH), the Liberty Hospitalist group graciously admitted patients to the hospital for the privately practicing Gates Hospitalist group (members of both the LH and NKCH medical staff) so that Gates Hospitalists could redeploy to assist NKCH. LH also granted a new Gates Hospitalist physician emergency privileges during this crisis.

Downtime Becomes Uptime

United by a common enemy and faced with shared adversity, the Liberty Hospital staff and physicians dedicated themselves to teamwork, enhanced professional interactions, and grace. The bridge across the digital divide was rebuilt, with experienced healthcare providers shepherding less experienced healthcare providers to the paper side of the divide. Once across the bridge, LH administrators remedied paper charting inefficiencies by decreasing nursing-to-patient ratios and limiting the number of inpatients.

The Electronic Health Record (EHR) is the most prominent reason physicians retire. None of the LH medical staff retired during the downtime with paper charting. During downtime, physicians had more time for clinical work because there was less clerical work. Physicians gained two minutes each day by not logging into a computer. They saved time with handwritten admission and discharge medication reconciliations. (In the EHR, there is a three-second delay following each medication reconciliation, and nearly every medication is listed twice as a home and hospital medication). Physicians enjoyed a reprieve from coding and documentation queries and pop-ups, although the local Hallmark distribution center might find a way to get pop-ups back on the paper chart.

The doorway to the hospital room became the "new patient portal." Direct interactions with patients and families replaced the social isolation associated with computer charting. Contemporaneous charting was timely, concise, and meaningful, replacing the EHR-associated delayed documentation and note bloat. Later into the cyber-attack, physicians were allowed to dictate H&Ps, consults, and discharge summaries. The cyber-attack provided transcriptionists with better employment opportunities.

Physician boots on the ground replaced telemedicine physician services. New physician orientation was faster because EHR training was unnecessary. Medical students replaced their styluses with pens and learned to chart on paper and write prescriptions. A daily debriefing and town hall meeting in the hospital auditorium replaced group emails and Zoom meetings.

Nursing and ancillary staff enjoyed more desktop space without the clutter of desktop computers, keyboards, and mice. Worksite safety improved with zero blue light exposure. Staff wellness improved with intermittent biceps strengthening exercises while carrying charts that got heavier each day the patient stayed in the hospital. The chart search replaced the Google search (first finding the chart and then finding what you needed in the chart). The staff's Latin abbreviations, spelling skills, and cursive handwriting improved (our 20th-century second-grade teachers are beaming with pride). Unfortunately, crime often begets crime, and there were isolated reports of looting of paper clips, rubber bands, chart dividers, a three-hole punch, a five-hole

punch, and even a desk on wheels from medical floors that had been closed.

Once the downtime extended into the new calendar year, we quickly adapted to date orders with the new calendar year. We also anticipate future benefits, such as referrals to our hand surgeon for carpal tunnel syndrome surgery.

Liberty Hospital was without computer access for several weeks, and during this time, paper charting was impervious to another cyber-attack. The LH staff could have succumbed to the Stockholm Syndrome (captives coming to love their captors), but we did not.

To move forward, we have to look at our steps along the path that led to hospital cyber-attacks.

The March to Electronic Health Record Interoperability

In 1996, the federal government took a step to protect electronic health records. The Health Insurance Portability and Accountability Act (HIPAA) provided (1) a privacy rule that established national standards to protect patient health information and (2) a security rule that set standards for the security of electronic patient health information.

In 2009, the federal government mobilized the hospital systems and increased the cadence of the march as it promoted EHR interoperability. The American Recovery and Reinvestment Act included three components of meaningful use:

1. Utilizing the EHR for meaningful use, such as e-prescribing
2. Exchanging health information to improve the quality of healthcare
3. Reporting clinical quality data

In 2016, the federal government drafted all remaining healthcare providers into the EHR interoperability effort. The 21st Century Cures Act (CURES) promoted electronic access, exchange, and use of health data. On May 1, 2020, the Office of National Coordinator (ONC) for Health Information Technology published the final CURES Act rule for interoperability and patient access. This rule required all healthcare providers to share electronic health information by October 6, 2022.

Halt the March, Identify the Enemy, and Define the Mission

Every successful military operation starts with identifying the enemy, evaluating their capabilities, and developing a clearly defined mission.

The enemy is the cyber-attacker, and their weapon is the internet. EHR interoperability requires an internet-based platform (open system) vulnerable to cyber-attacks. Interoperability places personal information, including our health records, financial information, insurance information, social security numbers, home addresses, and phone numbers, in clear and present danger.

It is time to define the hospital's primary mission in the context of the risks and benefits of EHR interoperability. Should the hospital's primary mission be to provide interoperability of electronic medical records for the federal government, third-party payers, and other healthcare systems? Or should the hospital's primary mission be to provide reliable, accessible care, and the best medical care while ensuring patient privacy?

A Paper Shield

In the Medieval Age, Don Quixote futilely fought windmills. In the Industrial Age, John Henry beat the steam engine but died immediately following his victory. Cyber-attacks threaten to bomb us from the Technology Age to the Pre-Technology Age of pen and paper. It is not a time to fight paper mills but to celebrate Arbor Day.

Hospitals must comply with federal requirements of meaningful use and interoperability that increase their risk of a cyber-attack. Hospitals' only option to decrease the risk of damage from a cyber-attack is to dedicate more resources to cybersecurity and cybersecurity insurance. Unfortunately, hospitals have limited resources for cybersecurity because federal, state, and commercial insurance reimbursement for healthcare services is decreasing while their costs for staff, supplies, and services are rising. Hospitals have to choose between providing computer care, and providing patient care.

The Nuclear Shield: An Open and Closed Case

In the 1983 fictional movie "War Games," a teenage computer geek inadvertently hacked into a government nuclear weapons website. His computer asked him, "Would you like to play a game?" The geek, thinking it was simply a game, started playing, and a series of events unfolded, after which a worldwide nuclear war nearly occurred. In November of 2007, the non-fictional computer worm Stuxnet exploited the vulnerabilities of Iran's nuclear program. The United States of America's nuclear arsenal has not been hacked in large part because our nuclear silos are on a closed system, an intranet rather than an internet-based system. This secure system provides our nuclear weapons with the highest level of security.

Cyber attacks on interoperable EHRs are a clear and present danger to patient's access to healthcare and personal information. It is time to recognize that hospitals are "mission critical" for healthcare in America. If our hospitals are to receive the same level of security that our nuclear silos receive, then our hospitals' EHRs should be on closed systems that are not interoperable and not accessible from outside the hospital. The only way to achieve this objective is by:

1. Revoking hospital EHR meaningful use requirements
2. Exempting hospitals from interoperability requirements
3. Requiring EHR vendors to offer closed/intranet EHR products to hospitals

Patients and physicians would benefit from the security of a closed hospital EHR system; however, there would be sacrifices, including:

- Loss of Interoperability
- Loss of the patient portal
- Termination of hospital telemedicine services
- Loss of remote access by medical staff
- Loss of e-prescribing

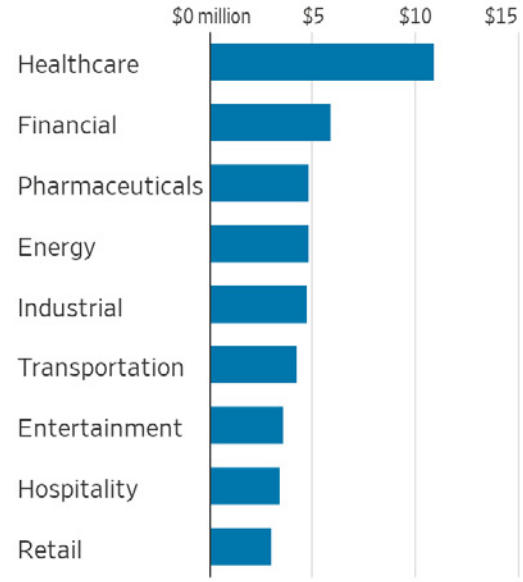
As long as hospital EHRs are interoperable, they are in clear and present danger of cyber-attacks. Having survived one of these hospital cyber-attacks, I strongly encourage our elected officials to reevaluate the risks and benefits of hospital EHR interoperability.

1 Picture = 1,000 Words

Liberty Hospital Determines Cyber-Security Incident Caused Patient Care Disruption

(December 19, 2023)

Hospital Ransom Hacks Highest Ever in 2023



Sources

1. "Internet Crime Report 2022." Federal Bureau of Investigation, 2022, www.fbi.gov.
2. "Hospitals could be one cyberattack away from closure." Axios, www.axios.com.
3. "Average duration of downtime after a ransomware attack at organizations worldwide from 1st quarter 2020 to 2nd quarter 2022." Statista, 2022, www.statista.com.
4. Bruce, Giles. "Hackers threaten to send SWAT teams to Fred Hutch patients' homes." Becker's HEALTH IT, 4 Jan. 2024, www.beckershospitalreview.com.
5. LaPoint, Jacqueline. "Healthcare Has Yet to Feel Full Impact of Physician Retirements." Revcycles Intelligence, 22 Mar. 2023, www.revcycleintelligence.com.
6. "The Health Insurance Portability and Accountability Act (HIPAA) of 1996." Pub. L. No. 104-191, 110 Stat. 1936.
7. "The American Recovery and Reinvestment Act of 2009." Pub. L. No. 111-5, 123 Stat. 115.
8. "The 21st Century Cures Act (CURES) of 2016." Pub. L. No. 114-255, 130 Stat. 1033.
9. Badham, John, director. War Games. United Artists, 1983.
10. "Stuxnet." 2007.

MM