

Ransomware Attacks Will Keep Coming — What Physician Leaders Should Do

By Lola Butcher

Ransomware attacks on healthcare facilities are expected to continue, and every organization should consider itself a target. Physician leaders should develop contingency plans for how their organizations can best care for patients if essential technologies — electronic medical record software, telephones, email, and others — are out of commission for an extended period of time.

KEY WORDS: Ransomware; physician leaders; information technology; cyberattack; patient safety; quality of care.

The pandemic's work-from-home movement was in full swing in late 2020 when a laptop a University of Vermont Medical Center (UVM) employee took home was infected by malware. When the computer plugged back into the UVM system on Oct. 28, it launched a ransomware attack and Stephen Leffler, MD, president and chief operating officer, faced a physician leader's nightmare.

"The cyberattack was much harder than the pandemic by far," Leffler said last fall in testimony before a congressional subcommittee investigating ransomware.

Leffler is one of hundreds of physician leaders who have dealt with an attack in recent years — and many more will face them in the future. "I think we have to assume this is going to continue to happen," says Mark P. Jarrett, MD, chair of the U.S. Healthcare and Public Health Sector Coordinating Council, a private-sector group that works with the federal government to protect critical healthcare infrastructure.

Information technology experts are responsible for defending against a cyberattack or limiting the damage when one occurs in their organizations. But physician leaders have an equally big job: planning for the possibility of an attack. "No matter how good the defense is, it could still happen," explains Jarrett, senior health advisor for Northwell Health. "And if it happens, what does that mean for clinical care in my institution?"

WHO IS AT RISK?

The crippling attack in February on Change Healthcare, a unit of United HealthGroup, one of the world's biggest healthcare companies, showed that no one is safe from ransomware and the U.S. healthcare sector is a favorite target.

Globally, more than 630 ransomware incidents attacked healthcare organizations in 2023, and 460 occurred in the United States, according to the U.S. Department of Health and Human Services.

The larger organizations — Scripps Health, Lurie Children's Hospital, CommonSpirit Health, Universal Health Services — get most of the attention, but ransomware thieves like healthcare organizations of all kinds.

Michael A. Puskarich, MD, an emergency physician and researcher at Hennepin Healthcare in Minneapolis, was part of a research team that reviewed healthcare ransomware attacks for the five-year period ending in 2021.¹ "In our data, about half of the attacks were on clinics," he reports. "Just because you're a small fish doesn't mean you're not at risk."

From the cybercriminals' perspective, UVM would have been a big fish, but the hook came up empty. No patient or employee data were seized and no ransom was paid.

Regardless, the malware encrypted the files and data on the system's 1,300 servers and about 5,000 desktop computers. For a while, UVM clinics did not know which patients had appointments, at what time, or for what reason. "I had to go on the news and say, 'If you are coming for an appointment today, bring everything you have with you to help us take care of you,'" Leffler says.

Because UVM's phone system is internet based, for the first two days after the attack, the system had no phone service. "We literally went to Best Buy and bought every walkie-talkie they had," Leffler says. "I asked our administrators to run lab results to the floors."

The electronic medical record (EMR) system was offline for 28 days. "Many of our young new doctors had never written paper orders, so we had to go back and teach them how to do that," he says. "We brought together our clinical

leaders from surgery, anesthesia, trauma, emergency medicine, obstetrics, medicine, and they met — sometimes twice-a-day — seven days a week for 28 days to decide how they could safely provide care..., what care could be safely delayed, and what care could be transferred out-of-state to other academic medical centers.”

Every computer needed to be wiped clean and then reimaged, a round-the-clock job that took weeks, with National Guard workers called in to help. More than 600 software applications across the enterprise were prioritized for restoration based on their clinical impact; full operation was not restored until January. The total cost of the ordeal, including cleaning and rebooting the system, lost revenue, and extra staff: \$65 million.

It could have been much worse, but for two important planning steps. First, UVM’s IT team was empowered to act quickly without taking time to alert system leaders. “When that attack first started, before our IT team even knew what was occurring, they made the decision to shut down our system,” Leffler explains. “That single move protected any patient care information from being released or any employee information from being released and was key to our overall action during the incident.”

Secondly, because the medical center had a good backup system for its servers, it did not have to pay the ransom to regain access to its data.

Many healthcare organizations are developing cyberattack-response plans, but many more have not yet devoted the time, effort, and resources that are required. “In over 90% of our institutions we are not really as well-prepared as we should be,” Jarrett says.

WHAT TO DO NOW

The most important thing for physician leaders to do is to convince all clinicians and other staff that preventing a cyberattack is essential for patient safety and quality of care. Prevention means being careful with email messages, email attachments, links, webpages, and passwords.

“You need to think of yourself as the first line of defense and you need to practice good cybersecurity hygiene because it is important for good clinical practice,” emergency physician Christian Dameff, MD, cautioned in a *Cybersecurity for the Clinician* video series presented by the Health Sector Coordinating Council Cybersecurity Working Group.

Dameff is co-director of the new UC San Diego Center for Health Care Cybersecurity. Researchers at the center, aided by a \$9.5 million federal grant, are working to identify early indicators of cybersecurity threats through simulated attacks.

Meanwhile, real attacks will continue, and Dameff rattles off their ramifications: “Medical devices can stop working or their settings can be corrupted so that they actually are dangerous to the patients. Strokes, trauma, cardiac, and

other services can be closed for admissions. Radiation and other treatments for cancer patients, including surgery, are delayed. Medical records about prescriptions, diagnoses, and therapies become inaccessible and some may be permanently lost. Research or lab clinical trial data can be lost. Payment systems are down. You’re unable to order and receive supplies. You are moved to a paper system temporarily, which causes enormous time lags, inefficiencies, and errors. Staff are furloughed.”

These challenges require thoughtful planning, not decisions made in the heat of the moment, he says.

Christopher Longhurst, MD, chief medical officer and chief digital officer at UC San Diego Health, encourages chief medical officers to partner with their chief information officers to prepare for the possibility of a cyber-disaster. “You have to understand and educate the executive team that a ransomware event is a disaster and that you have to prepare for it,” he explains.

Conducting tabletop exercises similar to those used to plan for active shooters and mass disasters helps leaders think through the issues that may arise.

“During our tabletop, there were things that came up that we hadn’t thought about,” Longhurst says. “How do you communicate if your email system is down? What are we going to say publicly? What do we want to tell our patients? Having an approach that you have agreed on beforehand is important because, a lot of times when you get into a crisis, the natural approach is to batten down the hatches, so you need to have a playbook.”

Jarrett suggests using scheduled EMR downtimes to conduct drills. “You have to work with all of the staff in the hospital — the laboratory, radiology, everybody — to see what you can do to keep things functioning for an extended period of time,” he says.

It’s the extended period of time that Leffler, the UVM president and COO, emphasizes. “We typically did a drill where we would have our EMR down for two days, which seemed like a really long time,” he explains. During the cyberattack, “we were down for 28 days and the things you need to do over 28 days are vastly different. I would recommend all hospitals or healthcare systems do a tabletop exercise to imagine what it would be like to be down for a month.”

Provider organizations can be affected by a ransomware attack even if their own organization is not the one hit. When a major health system in San Diego was laid low by a ransomware attack in 2021, two academic urban emergency departments (EDs) unaffiliated with the attacked system felt the blow, according to a *JAMA Network Open* article written by Dameff and several colleagues.²

In the month that included the attack and recovery, the two EDs recorded:

- Average daily census of more than 251 patients, compared to 218 in the month before the attack.

- A mean of 2,354 ambulance arrivals, compared to 1,741.
- Three-hundred-sixty patients left without being seen, more than double the month before the attack.
- Median door-to-room time of 31 minutes, compared to 21 minutes.
- Median total length of stay for admitted patients of 822 minutes compared to 614 minutes.

Those two academic medical centers typically account for only about 11% of the regional inpatient discharges, which means other hospitals in the area were likely also affected.

“It reverberated throughout our entire community,” Longhurst says. “We want the federal government, the state government, the regulators, and others to think about a ransomware attack as a mass casualty event because it’s a major regional disaster.”

Doing so could mean a government-supported formal regional response prepared in case an organization is attacked.

“In a lot of these cases, hospitals are being attacked by nation-state threat actors, and these cybergangs are using software that is almost impossible to defend against,” Longhurst says. “We have seen the FBI and NASA infiltrated by these attacks. If best practices are being put in place and there is still a breach by a state actor, there should be some protection.”

PHYSICIANS PROTECTING PATIENTS

While elected and regulatory leaders decide how to deal with the burgeoning ransomware crisis, physician leaders around the country are taking steps to protect their own patients.

Stroke patients, for example, are particularly vulnerable to delays in care, which can happen when cyberattacks force stricken hospitals to divert ambulances away from their emergency departments. The two EDs in the San Diego analysis saw the number of confirmed strokes more than double — from 22 in the four weeks before the attack on their neighboring health system to 47 in the four weeks including the attack and recovery period. ED stroke codes increased from 49 in the four weeks before the attack to 103, and acute stroke treatments more than doubled.

In addition to understanding and supporting the organization-wide contingency plan for a cyberattack,

clinical leaders may need to make contingency plans for their own patients in particular, says Mouhammad A. Jumaa, MD, neurosciences service line chief at ProMedica health system in Toledo, Ohio.

Jumaa is medical director of the ProMedica Stroke Network, responsible for telestroke coverage to 21 community hospitals. When a patient suffers a stroke, a quick diagnosis and treatment are critical. That quick diagnosis relies on four technologies that could be disrupted by a ransomware attack: emergency medical services (EMS) dispatch and communication software for transport; artificial intelligence-powered imaging software for stroke identification; telemedicine software; and the electronic medical record system.

“It’s important to establish an internal plan for a stroke network to change some of what we do to be able to accommodate patients,” he says.

Those plans could include pivoting to HIPAA-compliant FaceTime or WhatsApp applications if telestroke software is offline; making sure EMS transport teams have radio equipment as a backup; and being prepared to send stroke specialists from the comprehensive stroke center to a community hospital if that’s what it takes to provide timely care.

Back at UVM, the health system’s IT department has taken steps to make it harder for malware to move through its computer network when another attack occurs. “We assume it is going to happen again,” Leffler told the congressional committee. “There are so many people trying.” ■

REFERENCES

1. Neprash HT, McGlave CC, Cross DA, *et al.* Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016–2021. *JAMA Health Forum.* 2022;3(12):e224873. <https://doi.org/10.1001/jamahealthforum.2022.4873>
2. Dameff C, Tully J, Chan TC, *et al.* Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. *JAMA Netw Open.* 2023;6(5):e2312270. <https://doi.org/10.1001/jamanetworkopen.2023.12270>

<https://doi.org/10.55834/plj.8756126942>

Copyright © 2024 by American Association for Physician Leadership®



Lola Butcher is a freelance healthcare journalist based in Missouri.