Experts say US hospitals are prone to cyberattacks

June 25 2024, by Rachana Pradhan, Kate Wells, Michigan Public, KFF Health News

In the wake of a debilitating cyberattack against one of the nation's largest health care systems, Marvin Ruckle, a nurse at an Ascension hospital in Wichita, Kansas, said he had a frightening experience: He nearly gave a baby "the wrong dose of narcotic" because of confusing paperwork.

Ruckle, who has worked in the neonatal intensive care unit at Ascension Via Christi St. Joseph for two decades, said it was "hard to decipher which was the correct dose" on the medication record. He'd "never seen that happen," he said, "when we were on the computer system" before the cyberattack.

A May 8 ransomware attack against Ascension, a Catholic health system with 140 hospitals in at least 10 states, locked providers out of systems that track and coordinate nearly every aspect of patient care. They include its systems for electronic health records, some phones, and ones "utilized to order certain tests, procedures and medications," the company said in a May 9 statement.

More than a dozen doctors and nurses who work for the sprawling health system told Michigan Public and KFF Health News that patient care at its hospitals across the nation was compromised in the fallout of the cyberattack over the past several weeks. Clinicians working for hospitals in three states described harrowing lapses, including delayed or lost lab results, medication errors, and an absence of routine safety checks via
technology to prevent potentially fatal mistakes.

Despite a precipitous rise in cyberattacks against the health sector in recent years, a weeks-long disruption of this magnitude is beyond what most health systems are prepared for, said John Clark, an associate chief pharmacy officer at the University of Michigan health system.

"I don't believe that anyone is fully prepared," he said. Most emergency management plans "are designed around long-term downtimes that are into one, two, or three days."

Ascension in a public statement May 9 said its care teams were "trained for these kinds of disruptions," but did not respond to questions in early June about whether it had prepared for longer periods of downtime.

Ascension said June 14 it had restored access to electronic health records across its network, but that patient "medical records and other information collected between May 8" and when the service was restored "may be temporarily inaccessible as we work to update the portal with information collected during the system downtime."

Ruckle said he "had no training" for the cyberattack.

**Back to Paper**

Lisa Watson, an intensive care unit nurse at Ascension Via Christi St. Francis hospital in Wichita, described her own close call. She said she nearly administered the wrong medication to a critically ill patient because she couldn't scan it as she normally would. "My patient probably would have passed away had I not caught it," she said.

Watson is no stranger to using paper for patients' medical charts, saying she did so "for probably half of my career," before electronic health records became ubiquitous in hospitals. What happened after the
cyberattack was "by no means the same."

"When we paper-charted, we had systems in place to get those orders to other departments in a timely manner," she said, "and those have all gone away."

Melissa LaRue, an ICU nurse at Ascension Saint Agnes Hospital in Baltimore, described a close call with "administering the wrong dosage" of a patient's blood pressure medication. "Luckily," she said, it was "triple-checked and remedied before that could happen. But I think the potential for harm is there when you have so much information and paperwork that you have to go through."

Clinicians say their hospitals have relied on slapdash workarounds, using handwritten notes, faxes, sticky notes, and basic computer spreadsheets—many devised on the fly by doctors and nurses—to care for patients.

More than a dozen other nurses and doctors, some of them without union protections, at Ascension hospitals in Michigan recounted situations in which they say patient care was compromised. Those clinicians spoke on the condition that they not be named for fear of retaliation by their employer.

An Ascension hospital emergency room doctor in Detroit said a man on the city's east side was given a dangerous narcotic intended for another patient because of a paperwork mix-up. As a result, the patient's breathing slowed to the point that he had to be put on a ventilator. "We intubated him and we sent him to the ICU because he got the wrong medication."

A nurse in a Michigan Ascension hospital ER said a woman with low blood sugar and "altered mental status" went into cardiac arrest and died
after staff said they waited four hours for lab results they needed to
determine how to treat her, but never received. "If I started having
crushing chest pain in the middle of work and thought I was having a big
one, I would grab someone to drive me down the street to another
hospital," the same ER nurse said.

Similar concerns reportedly led a travel nurse at an Ascension hospital in
Indiana to quit. "I just want to warn those patients that are coming to any
of the Ascension facilities that there will be delays in care. There is
potential for error and for harm," Justin Neisser told CBS4 in
Indianapolis in May.

Several nurses and doctors at Ascension hospitals said they feared the
errors they've witnessed since the cyberattack began could threaten their
professional licenses. "This is how a RaDonda Vaught happens," one
nurse said, referring to the Tennessee nurse who was convicted of
criminally negligent homicide in 2022 for a fatal drug error.

Reporters were not able to review records to verify clinicians' claims
because of privacy laws surrounding patients' medical information that
apply to health care professionals.

Ascension declined to answer questions about claims that care has been
affected by the ransomware attack. "As we have made clear throughout
this cyber attack which has impacted our system and our dedicated
clinical providers, caring for our patients is our highest priority," Sean
Fitzpatrick, Ascension's vice president of external communications, said
via email on June 3. "We are confident that our care providers in our
hospitals and facilities continue to provide quality medical care."

The federal government requires hospitals to protect patients' sensitive
health data, according to cybersecurity experts. However, there are no
federal requirements for hospitals to prevent or prepare for cyberattacks
that could compromise their electronic systems.

**Hospitals: 'The No.1 target of ransomware'**

"We've started to think about these as public health issues and disasters on the scale of earthquakes or hurricanes," said Jeff Tully, a co-director of the Center for Healthcare Cybersecurity at the University of California-San Diego. "These types of cybersecurity incidents should be thought of as a matter of when, and not if."

Josh Corman, a cybersecurity expert and advocate, said ransom crews regard hospitals as the perfect prey: "They have terrible security and they'll pay. So almost immediately, hospitals went to the No. 1 target of ransomware."

In 2023, the health sector experienced the largest share of ransomware attacks of 16 infrastructure sectors considered vital to national security or safety, according to an FBI report on internet crimes. In March, the federal Department of Health and Human Services said reported large breaches involving ransomware had jumped by 264% over the past five years.

A cyberattack this year on Change Healthcare, a unit of UnitedHealth Group's Optum division that processes billions of health care transactions every year, crippled the business of providers, pharmacies, and hospitals.

In May, UnitedHealth Group CEO Andrew Witty told lawmakers the company paid a $22 million ransom as a result of the Change Healthcare attack—which occurred after hackers accessed a company portal that didn't have multifactor authentication, a basic cybersecurity tool.

The Biden administration in recent months has pushed to bolster health
care cybersecurity standards, but it's not clear which new measures will be required.

In January, HHS nudged companies to improve email security, add multifactor authentication, and institute cybersecurity training and testing, among other voluntary measures. The Centers for Medicare & Medicaid Services is expected to release new requirements for hospitals, but the scope and timing are unclear. The same is true of an update HHS is expected to make to patient privacy regulations.

HHS said the voluntary measures "will inform the creation of new enforceable cybersecurity standards," department spokesperson Jeff Nesbit said in a statement.

"The recent cyberattack at Ascension only underscores the need for everyone in the health care ecosystem to do their part to secure their systems and protect patients," Nesbit said.

Meanwhile, lobbyists for the hospital industry contend cybersecurity mandates or penalties are misplaced and would curtail hospitals' resources to fend off attacks.

"Hospitals and health systems are not the primary source of cyber risk exposure facing the health care sector," the American Hospital Association, the largest lobbying group for U.S. hospitals, said in an April statement prepared for U.S. House lawmakers. Most large data breaches that hit hospitals in 2023 originated with third-party "business associates" or other health entities, including CMS itself, the AHA statement said.

Hospitals consolidating into large multistate health systems face increased risk of data breaches and ransomware attacks, according to one study. Ascension in 2022 was the third-largest hospital chain in the
U.S. by number of beds, according to the most recent data from the federal Agency for Healthcare Research and Quality.

And while cybersecurity regulations can quickly become outdated, they can at least make it clear that if health systems fail to implement basic protections there "should be consequences for that," Jim Bagian, a former director of the National Center for Patient Safety at the Veterans Health Administration, told Michigan Public's Stateside.

Patients can pay the price when lapses occur. Those in hospital care face a greater likelihood of death during a cyberattack, according to researchers at the University of Minnesota School of Public Health.

Workers concerned about patient safety at Ascension hospitals in Michigan have called for the company to make changes.

"We implore Ascension to recognize the internal problems that continue to plague its hospitals, both publicly and transparently," said Dina Carlisle, a nurse and the president of the OPEIU Local 40 union, which represents nurses at Ascension Providence Rochester.

At least 125 staff members at that Ascension hospital have signed a petition asking administrators to temporarily reduce elective surgeries and nonemergency patient admissions, like under the protocols many hospitals adopted early in the COVID-19 pandemic.

Watson, the Kansas ICU nurse, said in late May that nurses had urged management to bring in more nurses to help manage the workflow. "Everything that we say has fallen on deaf ears," she said.

"It is very hard to be a nurse at Ascension right now," Watson said in late May. "It is very hard to be a patient at Ascension right now."

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.