# Hospital chain attack part of ongoing cybersecurity concerns

October 7 2022, by KATHLEEN FOODY and KIMBERLEE KRUESI


The MercyOne Des Moines Medical Center campus is seen, Thursday, Oct. 6, 2022, in Des Moines, Iowa. Diverted ambulances. Cancer treatment delayed. Electronic health records offline. These are just some of ripple effects of an apparent cyberattack on the major nonprofit health system that disrupted operations throughout the U.S. Meanwhile, The Des Moines Register said the incident occurred Monday, Oct. 3, 2022, and forced the diversion of five ambulances from the emergency department of the city's Mercy One Medical Center to other medical facilities. Credit: AP Photo/Charlie Neibergall

Diverted ambulances. Cancer treatment delayed. Electronic health records offline. These are just some of ripple effects of an apparent cyberattack on a major nonprofit health system that disrupted operations throughout the U.S.

While CommonSpirit Health confirmed it experienced an "IT security issue" earlier this week, the company has remained mum when pressed for more details about the scope of the attack. The health system giant has 140 hospitals in 21 states. As of Thursday, it's still unknown how many of its 1,000 care sites that serve 20 million Americans were affected.

Despite the lingering questions, the incident underscores the growing concerns surrounding ransomware attacks on health care systems with patient care at stake.

In Tacoma, Washington, Mark Kellogg told KING-TV that his wife, Kathy, had been scheduled to get a cancerous tumor on her tongue removed on Monday, but the procedure was put off several days because of the cyberattack. Virginia Mason Franciscan Health's parent company is CommonSpirit Health.

"Everything we do today is all on a computer, and without it you're back to the stone age writing on a tablet," Kellogg said.

In Iowa, the Des Moines Register reported that the incident forced the diversion of five ambulances from the emergency department of the city's MercyOne Medical Center to other medical facilities.

The incident forced both MercyOne and VMFH to take certain IT systems offline—including patients' electronic health records—as a

precaution.

Brett Callow, a threat analyst with cybersecurity provider Emsisoft, said the incident could be "the most significant attack on the health care sector to date" if all CommonSpirit hospitals and other facilities were affected.

Emsisoft has tracked at least 15 health care systems in the U.S. affected by ransomware this year, which manage more than 60 hospitals. Callow said data was stolen in 12 of the 15 instances, adding that those are almost surely undercounts as some ransomware attacks aren't widely reported.

Callow said one of the largest known attacks within health care came in September 2020 when a ransomware attack struck all 250 health care facilities owned by Universal Health Services.

CommonSpirit's incident could exceed that, depending on how many of its facilities were hit. That could mean the company faces large financial costs to get through the incident and recover.

Callow cited the loss of more than $100 million reported by Scripps Health tied to a 2021 ransomware attack that affected its five hospitals in California as an example.

Asked for more information on the incident and its effects on Thursday, a spokesperson for CommonSpirit said the health system could not provide more details.

The most worrying effect of any substantial attack on healthcare is on patients, Callow said.

"I've seen reports that at least one of the impacted hospitals had to divert

ambulances to other facilities and that delay in getting people the care they need could obviously represent a risk to the lives of patients," he said. "Beyond that, these incidents can have a long-term impact on patient outcomes—delaying treatments, for example."

In 2020, the FBI and other federal agencies warned that they had credible information that cybercriminals could unleash a wave of data-scrambling extortion attempts against U.S. hospitals and health care providers.

That's because ransomware criminals are increasingly stealing data from their targets before encrypting networks, using it for extortion. They often sow the malware weeks before activating it, waiting for moments when they believe they can extract the highest payments.

Health care is classified by the U.S. government as one of 16 critical infrastructure sectors Health care providers are seen as ripe targets for hackers.

If patient data is accessed, health care providers are required by law to notify the Department of Health and Human Services.