A CYBERATTACK FORCES A BIG US HEALTH SYSTEM TO DIVERT AMBULANCES AND TAKE RECORDS OFFLINE - ASSOCIATED PRESS

Posted on May 11, 2024 by JOHN HANNA, TOM MURPHY and KATHLEEN FOODY | Associated Press

Photo: Buildings stand in the Milwaukee skyline on Sept. 6, 2022, in Milwaukee

A cyberattack on the Ascension health system operating in 19 states across the U.S. forced some of its 140 hospitals to divert ambulances, caused patients to postpone medical tests and blocked online access to patient records.

An Ascension spokesperson said it detected "unusual activity" Wednesday on its computer network systems. Officials refused to say whether the non-profit Catholic health system, based in St. Louis, was the victim of a ransomware attack or whether it had paid a ransom, and it did not immediately respond to an email seeking updates.

But the attack had the hallmarks of a ransomware, and Ascension said it had called in Mandiant, the Google cybersecurity unit that is a leading responder to such attacks. Earlier this year, a cyberattack on Change Healthcare disrupted care systems nationwide, and the CEO of its parent, UnitedHealth Group Inc., acknowledged in testimony to Congress that it had paid a ransom of $22 million in bitcoin.

Ascension said that both its electronic records system and the MyChart system that gives patients access to their records and allows them to communicate with their doctors were offline.

"We have determined this is a cybersecurity incident," the national Ascension spokesperson's statement said. "Our investigation and restoration work will take time to complete, and we do not have a timeline for completion."

To prevent the automated spread of ransomware, hospital IT officials typically take electronic medical records and appointment-scheduling systems offline. UnitedHealth CEO Andrew Witty told congressional committees that Change Healthcare immediately disconnected from other systems to prevent the attack from spreading during its incident.

The Ascension spokesperson's latest statement, issued Thursday, said ambulances had been diverted from "several" hospitals without naming them.

In Wichita, Kansas, local news reports said the local emergency medical services started diverting all ambulance calls from its hospitals

there Wednesday, though the health system's spokesperson there said Friday that the full diversion of ambulances ended Thursday afternoon.

The EMS service for Pensacola, Florida, also diverted patients from the Ascension hospital there to other hospitals, its spokesperson told the Pensacola News Journal.

And WTMJ-TV in Milwaukee reported that Ascension patients in the area said they were missing CT scans and mammograms and couldn't refill prescriptions.

Connie Smith, president of the Wisconsin Federation of Nurses and Health Professionals, is among the Ascension providers turning to paper records this week to cope. Smith, who coordinates surgeries at Ascension St. Francis Hospital in Milwaukee, said the hospital didn't cancel any surgical procedures and continued treating emergency patients.

But she said everything has slowed down because electronic systems are built into the hospital's daily operations. Younger providers are often unfamiliar with paper copies of essential records and it takes more time to document patient care, check the results of prior lab tests and verify information with doctors' offices, she said.

Smith said union leaders feel staff and service cutbacks have made the situation even tougher. Hospital staff also have received little information about what led to the attack or when operations might get closer to normal, she said.

"You're doing everything to the best of your ability but you leave feeling frustrated because you know you could have done things faster or gotten that patient home sooner if you just had some extra hands," Smith said.

Ascension said its system expected to use "downtime" procedures "for some time" and advised patients to bring notes on their symptoms and a list of prescription numbers or prescription bottles with them to appointments.

Cybersecurity experts say ransomware attacks have increased substantially in recent years, especially in the health care sector. Increasingly, ransomware gangs steal data before activating data-scrambling malware that paralyzes networks. The threat of making stolen data public is used to extort payments. That data can also be sold online.

"We are working around the clock with internal and external advisors to investigate, contain, and restore our systems," the Ascension spokesperson's latest statement said.

The attack against Change Healthcare earlier this year delayed insurance reimbursements and heaped stress on doctor's offices around the country. Change Healthcare provides technology used by doctor offices and other care providers to submit and process billions of insurance claims a year.

It was unclear Friday whether the same group was responsible for both attacks.

Witty said Change Healthcare's core systems were now fully functional. But company officials have said it may take several months of analysis to identify and notify those who were affected by the attack.

They also have said they see no signs that doctor charts or full medical histories were released after the attack. Witty told senators that UnitedHealth repels an attempted intrusion every 70 seconds.

A ransomware attack in November prompted the Ardent Health Services system, operating 30 hospitals in six states, to divert patients from some of its emergency rooms to other hospitals while postponing certain elective procedures.

—

Murphy reported from Indianapolis and Foody reported from Chicago.