Ransomware attack prompts multistate hospital chain to divert some emergency room patients elsewhere

November 28 2023, by JONATHAN MATTISE and JAKE BLEIBERG

Staff at The University of Kansas Health System St. Francis campus are seen on the first level of the hospital on Nov. 29, 2022, in Topeka, Kan. The University of Kansas Health System-St. Francis Campus in Topeka is on “divert status” because of a Nov. 23, 2023, cyber attack. Debbie Cluck, a spokeswoman, said it affects ambulance and that the emergency room is open. The disruption is sending patients flooding into the city's other hospital. Credit: Evert Nelson/The

Topeka Capital-Journal via AP

A ransomware attack has prompted a health care chain that operates 30 hospitals in six states to divert patients from some of its emergency rooms to other hospitals while postponing certain elective procedures.

Ardent Health Services said it took its network offline after the Nov. 23 cyberattack, adding in a statement that it suspended user access to information technology applications such as software used to document patient care.

By Tuesday afternoon, more than half of Ardent's 25 emergency rooms had resumed accepting some patients by ambulance or by fully lifting their "divert" status, Ardent spokesperson Will Roberts said. Divert status means hospitals have asked ambulances to take people needing emergency care to other nearby facilities. Roberts said hospitals nationwide have at times used divert status during flu season, COVID-19 surges, natural disasters and large trauma events.

The company said it could not yet confirm the extent of any compromised patient health or financial information. It reported the issue to law enforcement and retained third-party forensic and threat intelligence advisers, while working with cybersecurity specialists to restore IT functions as quickly as possible. There was no immediate timeline for resolving the problems.

Based in the Nashville, Tennessee, suburb of Brentwood, Ardent owns and operates 30 hospitals and more than 200 care sites with upwards of 1,400 aligned providers in Oklahoma, Texas, New Jersey, New Mexico, Idaho and Kansas.

Ardent said each hospital is still providing medical screenings and stabilizing care to patients arriving at emergency rooms.

In Amarillo, Texas, William Spell said he and his mother have had flu-like symptoms for days but couldn't make a doctor's appointment through an online patient portal because of the cyberattack.

"We are trying to figure out other options as to what to do next," said Spell, 34.

BSA Health System—the Ardent umbrella provider for Spell's clinic and other facilities in the city—said it was working to restore its patient portal and system for video doctors' visits. Spell said his doctor's office could not tell him how long the outage might last and recommended trying an urgent care clinic.

"That's just something we cannot do because urgent cares charge a lot of money just to walk through the door and be seen by a doctor," Spell said. "There's no way we can afford that."

Ardent says it is still seeing patients in its clinics and is contacting them if rescheduling is necessary.

Several hospitals in Albuquerque, New Mexico, within Ardent's Lovelace Health System have continued to divert some patients needing emergency care to other hospitals, Lovelace spokesperson Whitney Marquez said. They also rescheduled elective and other non-urgent surgeries.

In Topeka, Kansas, a hospital spokesperson confirmed the attack put the University of Kansas Health System-St. Francis on divert status. Meanwhile, the city's other hospital, Stormont Vail, said it increased weekend staffing after patient volume began growing Friday.

The University of Kansas Health System St. Francis, 1700 S.W. 7th St. exterior shown on Aug. 5, 2021, in Topeka, Kan. The University of Kansas Health System-St. Francis Campus in Topeka is on “divert status” because of a Nov. 23, 2023, cyber attack. Debbie Cluck, a spokeswoman, said it affects ambulance and that the emergency room is open. The disruption is sending patients flooding into the city's other hospital. Credit: Evert Nelson/The Topeka Capital-Journal via AP

There was no immediate claim of responsibility for the attack. Ransomware criminals do not usually admit to an attack unless the victim refuses to pay.

"The attack against Ardent Health is both egregious and quickly

becoming the norm," said analyst Allan Liska at the cybersecurity firm Recorded Future.

While some groups won't attack hospitals, "they are greatly outnumbered by those who will and with the number of ransomware groups growing every day, the percentage who won't attack hospitals is constantly decreasing," Liska said.

Even when health care providers don't pay, ransomware groups can sell patient data, Liska added.

The attacks also take a toll on hospitals around those that were targeted, said Dr. Christian Dameff, co-director of the Center for Healthcare Cybersecurity at the University of California, San Diego.

He described being in a "cyber blast radius" two years ago while working as an emergency room physician at a hospital near one that was attacked. He said patients waited longer for care and for beds if they needed to be admitted.

What is particularly problematic is when a targeted hospital provides specialized care, including for trauma and stroke patients. If they are lucky, another suitable hospital is nearby. "But in certain areas, especially rural and critical access areas, you can have a prolonged transport time because of diversions," said Dameff, who described the issue in a paper earlier this year in JAMA.

A recent global study by the cybersecurity firm Sophos found nearly two-thirds of health care organizations were hit by ransomware attacks in the year ending in March, double the rate from two years earlier but dipping slightly from 2022.

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. Sophos found data theft occurred in one in three ransomware attacks on health care organizations.

Analyst Brett Callow at the cybersecurity firm Emsisoft said 25 U.S. health care systems with 290 hospitals were hit last year while this year the number is 36 with 128 hospitals. Not all hospitals within the systems may have been impacted, and not all equally, he said.

"The fact that nobody appears to have yet died is partly due to luck," Callow added.

Most ransomware syndicates are run by Russian speakers based in former Soviet states, beyond the reach of U.S. law enforcement, though some "affiliates" who do the grunt work of infecting targets and negotiating ransoms live in the West.