PRO CYBER NEWS

Smaller Medical Providers Get Burned by Ransomware

Cyberattacks are pummeling doctors, dentists and community hospitals around the U.S., causing some to turn away patients and others to shut down

Campbell County Health, which operates a 90-bed community hospital in Wyoming, was hit by a cyberattack. PHOTO: CAMPBELL COUNTY HEALTH

By Adam Janofsky

Oct. 6, 2019 9:00 am ET

Andy Fitzgerald, chief executive of a community health system in Wyoming, was visiting his son in Georgia last month when he received a distressing text message from his chief operating officer: Their company had been hit by a cyberattack.

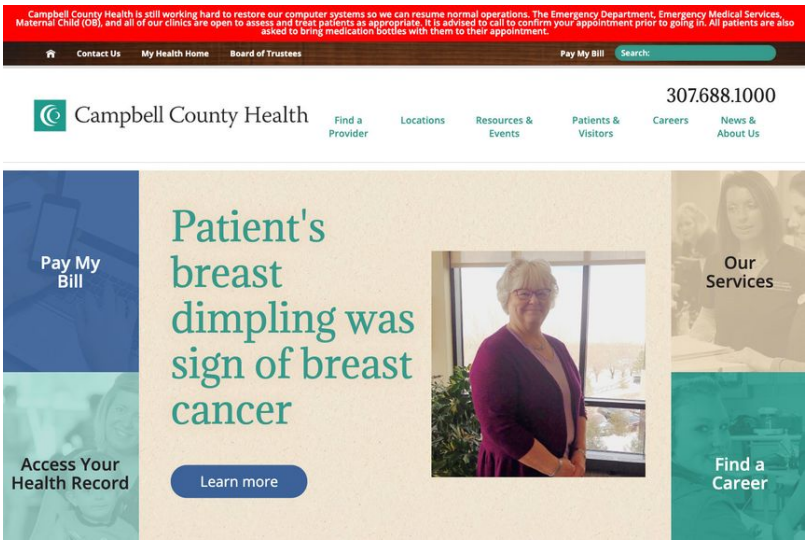
Hackers had locked up sensitive patient information and medical devices at Campbell County Health and demanded a ransom.

"My initial thought was, 'Oh crap,'" said Mr. Fitzgerald, who declined to say whether he paid the demand.

In the days after the attack, the health system, which operates a 90-bed community hospital and other facilities, was forced to cancel services including radiology, endocrinology and respiratory

therapy. The organization transferred patients to hospitals as far away as South Dakota and Denver. Cash registers, email and fax were unavailable. Doctors had to resort to pen and paper to document medical conditions, and with prescription records inaccessible, patients were asked to bring medication bottles to visits.

Employees have worked around the clock in the past few weeks to restore services, which are mostly back to normal, he said.



A warning is displayed at the top of Campbell County Health's website. PHOTO: CAMPBELL COUNTY HEALTH

Cyberattacks like this are pummeling doctors, dentists and community hospitals around the country, causing some to turn away patients and others to close their doors permanently.

Health organizations are an attractive target for cybercrime thanks to their valuable medical and billing information, said Jennifer Barr, a health-care analyst at Moody's Corp. The data can be sold for insurance-fraud purposes or it can be locked up and used to extort money from the affected health organization, she said.

Smaller health-care organizations are at greater risk because they generally don't have the resources for robust security tools and might not have a dedicated cybersecurity specialist to monitor and patch their systems, Ms. Barr said.

Last year, about 57% of medical practices in the U.S. had 10 or fewer physicians and about 15% were run by solo practitioners, according to the American Medical Association.

Three Alabama hospitals have been operating under emergency procedures since a cyberattack on Oct. 1, spokesman Bradley Fisher said Friday. The hospitals—DCH Regional, Northport and Fayette—are part of the same system and share IT resources.

"Everybody is familiar with [the emergency procedures] but you obviously don't want to do it for days," Mr. Fisher said. There is no forecast for when the hospitals will be functioning

normally, he said.

Like at the Wyoming health system, email is down and doctors are keeping written notes after patient visits. IT staff is working around the clock on eight-hour rotations, Mr. Fisher said, and about 60 nurse managers, department directors and other top administrators gather with the chief operating officer four times a day to go over technology and operational updates.

The hospital system is encouraging nonemergency patients to seek assistance from other providers.

In August, the American Dental Association said that hundreds of dental practices were affected by a ransomware attack that month against two dental-focused technology providers. The incident locked dentists out of their data but patient information is believed to be uncompromised, Brenna Sadler, director of membership and communications for the Wisconsin Dental Association, said in an email.

A Wisconsin dentist who asked not to be named said she has been "overwhelmed dealing with the incident [and] there are more repercussions than one might assume." She declined to give details.

After a ransomware attack, companies typically conduct digital forensic investigations to make sure systems and data are no longer vulnerable. Some equipment might have to be replaced and if backup data is outdated or encrypted, rebuilding files can be expensive and lengthy.

Some small health-care organizations don't have the money to bounce back from a cyberattack, said Linn Freedman, head of the privacy and cybersecurity practice at law firm Robinson & Cole LLP.

A ransomware incident in August is forcing Wood Ranch Medical in Simi Valley, Calif., to close its doors Dec. 17, according to a note posted on its website.

"Unfortunately, the damage to our computer system was such that we are unable to recover the data stored there and, with our backup system encrypted as well, we cannot rebuild our medical records," the note reads. "As much as I have enjoyed providing medical care to you, I will not be able to attend to you professionally after that date."

The statement is unsigned; the practice is run by Shayla Kasel, a family medicine doctor, who didn't respond to requests for comment.

Brookside ENT and Hearing Center in Battle Creek, Mich., permanently closed its doors in April after a ransomware attack, according to a receptionist reached by phone shortly after the incident. All of the company's electronic data was made inaccessible after it decided not to pay a ransom, and the practice stayed open for a short time to refer patients to other health providers, she said.

A voicemail response for one Brookside doctor says he is retired and no longer seeing patients.

Write to Adam Janofsky at adam.janofsky@wsj.com