Cybersecurity: Ransomware attacks shut down clinics, hospitals

OCT 4, 2019

Andis Robeznieks
Senior News Writer

What's the news: October is National Cybersecurity Awareness Month and it arrives not a moment too soon. Ransomware attacks across all industries grew by 118% in the first quarter of the year, according to the August 2019 McAfee Labs Threat Report, and recent news reports reveal that health care-related computer systems are becoming an increasingly popular target for cyber criminals.

The threat is global in scope. Recent victims include the DCH Regional Health System, a three-hospital public safety-net provider based in Tuscaloosa, Alabama, and two large health systems in southwest Australia.

Why it matters for patients and physicians: Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.

Wood Ranch Medical, a clinic in Simi Valley, California, suffered a ransomware attack this summer, and has announced that it will close in December. "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," a clinic news release said.

Earlier this year, Brookside ENT and Hearing Center, based in Battle Creek, Michigan, shut down after it lost years of patient records following practice owners' refusal to pay a ransom.

The DCH system in Alabama discovered the cyberattack against it on Oct. 1, and announced it was not taking new patients but was able to provide critical services and move ahead with outpatient procedures and surgeries scheduled for Oct. 4. Patients with scheduled hospital procedures and tests were urged to call first. Patients with nonemergency medical needs were "encouraged to seek

assistance from other providers," a DCH news release said.

What's next: The AMA has also developed tips and advice on protecting your computers and network to keep your patient health records and other data safe from cyberattacks.

You should download these cybersecurity resources and share them with your staff and IT:

> How to improve your cybersecurity practices.
> Cybersecurity checklist for office computers.
> Protect your practice and your patients from cybersecurity threats.

An AMA physician cybersecurity survey found that physicians frequently rely on their IT vendors to handle their system's security. The survey also found that compliance with the Health Insurance Portability and Accountability Act is not enough to protect records.

Training staff to recognize suspicious emails remains one of the most effective tools for preventing cyberattacks. "Even with all the sophisticated attack techniques being developed, attackers are still highly dependent on human interaction and social engineering," the McAfee Labs report states.

Additionally, health care and security experts have developed a set of useful materials to help guard your entire medical practice against cyberattacks. These materials have been designed with small to medium-sized medical practices in mind.

The main document, "Health Industry Cybersecurity Practices," explores the five most relevant and current threats to physician offices and recommends 10 cybersecurity practices to help mitigate these threats. Two technical volumes (one and two) provide the "how" so physicians and office administrators can implement these practices in their small, medium or large health care organizations.