Cybercrime

Health care takes a hit.

September 4, 2017 By Kate Ferguson

When people think of currency, they usually picture a stack of bills. But economic trends show that patients' names, birth dates, insurance policy numbers, diagnosis codes and billing information mined from electronic health care records (EHRs) are worth up to 10 times more to shady entrepreneurs than a bunch of Benjamins, according to Experian, a global information service.

In 2015, in the biggest crime of its kind that year, the giant health care provider Anthem got hacked by thieves who stole the EHRs of 78.8 million of its customers. Soon, CareFirst BlueCross BlueShield and the UCLA Health Systems suffered the same fate. Then, in 2016, officials at Hollywood Presbyterian Medical Center, a private hospital in Los Angeles, shut down the facility's computer system for one week after hackers infected its computers with malware and locked administrators out of the health management system. (To regain access to the facility's computers, officials paid hackers a ransom of 40 Bitcoins, a sum equivalent to about $17,000.)

What's more, it's expected that these kinds of cyberattacks will persist because health care systems are notoriously vulnerable. One report notes that the health care industry lags "behind other industries in protecting its infrastructure and electronic protected health information." This is largely because the health care administrators who create budgets for information security processes and protocols are largely unaware of how to properly train their staff to protect networks in facilities where mobile workstations, unattended terminals, medical devices and wireless entry points are prime targets.

With the information gleaned from these sources, cybercriminals can buy or sell medical equipment or drugs, file fraudulent claims and engage in other schemes that can net them millions of dollars. Additionally, thieves can alter research information or health records and harm patients.

Many experts agree that digitization improves the quality and efficiency of health care. But there's a cost attached to this technology. Besides the threat hackers pose to cybersecurity in health care organizations, internet rogues also threaten mobile applications, such as glucose monitors, that people use to transmit sensitive health information over a device or network. "Smartphones and other portable devices are among the easiest attack vectors for hackers," says Ondrej Krehel, the CEO and founder of LIFARS, a digital forensics and cybersecurity intelligence firm based in New York City. "Just because we don't see many high-level cases in the press yet, it doesn't mean that it is not happening. We need to emphasize that these devices hold the key to our lives—both

corporate and individual. Because they are always close to us, in our pockets, users experience a false perception of security.”

How to resolve this complex issue? Educate and train hospital staff about the ways hackers initiate cyberattacks, experts suggest. In addition, protect information and establish security policies in health care facilities and doctors’ offices too.
