March 8, 2017

Cyber criminals follow the money ... to your health care data

Medical care providers, patients unprepared for savvy hackers who are zeroing in on lucrative health data

INFOGRAPHIC BY RODIKA TOLLEFSON, THIRDCERTAINTY

Criminals know there are dollars in data and that monetizing medical records is a lucrative pastime.

This trend could foreshadow the next evolution of medical identity fraud. Cyber criminals could sell medical identities to uninsured or underinsured individuals, peddle pharmaceuticals online, obtain and resell expensive medical equipment, or simply file insurance claims by matching up stolen patient and provider identities.

This monetization is in the early stages, yet it's easy to see how even an "offline" scenario could be adapted to cyberspace.

Related: *Cure for digital attacks on health care sector is elusive*

Here are some of the factors playing into these scenarios:

• Vast numbers of medical records from data breaches are available for sale on the Dark Web. These include identities of medical providers and billing information.

• More data is primed for breaches. Consider that 19.2 million

Americans (under age 65) became newly insured through the Affordable Care Act and the majority of health records are now electronic.

• A Ponemon Institute study, measuring the privacy and security of health care data, found that criminal attacks grew 125 percent since 2010, becoming the leading cause of data breaches.

• The billing system, both in the public and private sectors, is constantly exploited.

• Patient authentication is not mandatory—it's easy to use a stolen identify to obtain services or to bill for a phantom patient. Patient authentication systems such as chip-enabled cards are cost-prohibitive.

• The growing trend in virtual care creates new ways for cyber criminals to set up a fake online medical service.

"[Medical identity] data is a richer record that ... can be sold for many different reasons and to many different people, says Ed Cabrera, chief security officer at global cybersecurity software company Trend Micro.

Because of this potential fragmentation, identifying new patterns in cyber criminals' monetization trends is difficult. On the surface, it may appear the criminals are sitting on the data for now. But that's not likely the case.

Since medical data has a long shelf life thieves don't have to rush to cash in big batches. Adam Levin, author of *Swiped: How to Protect Yourself in a World Full of Scammers, Phishers, and Identity Thieves,* says this data is like having money in the bank.

"They will use it at their leisure," he says. "It is inevitable it will be used, but the timing is at the convenience of the thief."

(Full disclosure: Levin also is the founder of CyberScout, which sponsors Third Certainty.)

Cyber criminals also are being patient because "they don't want to tip their hand to law enforcement," says Ponemon Institute founder and chairman Larry Ponemon.

"They might do small things, but do it over a long period of time," he says.

New schemes on horizon

A recent report by Accenture Consulting found that 35 percent of victims reporting medical identity fraud had their identities

used for fraudulent billing and 26 percent, for fraudulent services. Ponemon Institute's earlier study found that 59 percent of victims' medical credentials were used for health care services and 56 percent, for prescription drugs or equipment.

Ponemon says it would be easy to buy and resell drugs or expensive medical equipment. He gives the example of a medical power scooter, which a criminal could obtain for the price of an insurance co-pay.

"The bad guys could sell them on eBay and monetize," Ponemon says. "And it may be harder to get caught than using a stolen credit card."

According to a health care industry report released by Trend Micro in February, stolen medical insurance ID cards are available underground for as little as $1, and full records of U.S. citizens, including medical information, for 99 cents, with bulk discounts available.

Jeff Leston, president of Castlestone Advisors LLC, says it's very easy to defraud the system.

"The crooks know what boxes need to get checked when a claim comes in," says Leston, whose company provides payment networks for preventing health insurance fraud. "And there's no verification that the patient was ever in the office."

It's especially easy to defraud Medicare because the Social Security number is part of the medical ID number.

"Anybody who's had their Social Security number compromised, their Medicare identity is stolen once they become eligible," he says.

Leston thinks telemedicine, especially virtual doctor visits, will become the next treasure trove of fraud.

"Not only do you not have (patients) coming to an office, but you could also submit claims for people all over the country," he says.

Other nefarious uses

Ponemon has discovered one potential niche through his research. Sophisticated cyber criminals are buying medical data to create dossiers on people, he says. They're capturing information from various databases—medical, tax records, personal finances, education, career, even causes and political leanings. Not unlike marketers do through various clearinghouses.

“Their mission is that this could come in handy at some point in time,” he says.

Cabrera notes that the criminal underground, like any other industry, is constantly innovating and reinvesting resources into areas that have a high return on investment. Which means there’s still much in store.

“There will be new lines of business created when it comes to health care attacks,” he says. “We’re going to continue to see more sophistication and automation for creating these different lines of business.”

More stories related to health data theft:

The issue with nixing Affordable Care Act that no one’s talking about

Encrypting medical records is vital for patient security

Internet of Things facilitates health care data breaches