NEWS MAY 27 2015, 8:05 PM ET

Electronic Medical Records Are Latest Target for Identity Thieves

by STEPHANIE GOSK

Despite high-profile hacks that have targeted high-profile retailers like Target and entertainment giant Sony Pictures, security experts are warning of a more prized target for identity thieves: medical records.

Eric Forseter, a father of three in Bethesda, Maryland, first got a letter in March from Anthem Inc. warning that his family's information may have been stolen in what the company has called a "very sophisticated attack." A few days later another letter arrived, this time from Premera Blue Cross.

"They didn't know exactly what was stolen or when it was stolen, only that it might be stolen," Forseter said.

Anthem, one of the nation's largest health insurance companies, said in February that hackers accessed a database containing 80 million records, and that Social Security numbers, names, dates of birth and medical insurance identification numbers were at risk.

It was followed by Premera Blue Cross, which announced a month later that it, too, was hacked, and health data for as many as 11 million people may have been compromised.

RELATED: IRS Says Thieves Stole Tax Info From 100,000 Taxpayers

The sensitive data in electronic medical records is all identity thieves need to take out loans, get passports, or make fraudulent tax returns, security experts say.

"You have all the recipes you need to perform identity theft," said Ben Feinstein, director of operations and development with the Dell SecureWorks Counter Threat Unit. "And with the digitization of the electronic medical records, these things are much easier to steal in bulk."

Ill-gotten identifiers like Social Security numbers are sold on the Internet — a recent visit to sites where the material is peddled found a fake passport for around $6,000. Full dossiers of basic personal information, called "fullz," typically go for around $30 per person, Feinstein said.

A study published in the Journal of the American Medical Association in April found that more than 29 million U.S. health records were compromised in data breaches between 2010 and 2013.

Not all of those breaches were the result of cyberattacks or led to stolen identities, but the journal found the numbers alarming enough to warn in an editorial that, “The personal health information of patients in the United States is not safe, and it needs to be."

A different study, released in 2015 by the Ponemon Institute, found that cases of medical identity theft have nearly doubled in the last five years, from 1.4 million adult victims to more than 2.3 million in 2014.

RELATED: IRS Breach Puts Spotlight on 'Costco of Cybercrime'

"Hospitals have traditionally underinvested in information technology," said John Halamka, who is in charge of computer security for Beth Israel Deaconess Medical Center in Boston. "So if you don't spend that much, you're not going to get the degree technological protection."

Experts say customers can also protect themselves by monitoring their credit reports and making sure that any health insurance statements don't contain procedures that no one in the family had.

Anthem has said no credit card or financial information was exposed in the hack and there is no evidence that medical test results or claims information was exposed. It said it has hired Mandiant, a cybersecurity firm, to find and fix problems with its systems.

Forseter said he was offered two years of free credit monitoring after his family's information was exposed. But he worries what happens after that — five, 10, 20 years down the road. His son and daughter's information may have been exposed in the two breaches, as well, Forseter said he was told.

"Their data is out there and they're very young," he said. "And that means that it's going to be sold over and over and over again."
