TimesRecordNews
Wichita Falls, Texas

The rise of medical identity theft

(MCT)

Monday, February 10, 2014

WASHINGTON — If modern technology has ushered in a plague of identity theft, one particular strain of the disease has emerged as most virulent: medical identity theft.

Last month, the Identity Theft Resource Center produced a survey showing that medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013. That is a far greater chunk than identity thefts involving banking and finance, the government and the military, or education. The U.S. Department of Health and Human Services says that since it started keeping records in 2009, the medical records of between 27.8 million and 67.7 million people have been breached.

The definition of medical identity theft is the fraudulent acquisition of someone's personal information — name, Social Security number, health insurance number — for the purpose of illegally obtaining medical services or devices, insurance reimbursements or prescription drugs.

"Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," said Pam Dixon, the founder and executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."

The Affordable Care Act has raised the stakes. One of the main concerns swirling around the disastrous rollout of federal and state health insurance exchanges last fall was whether the malfunctioning online marketplaces were compromising the confidentiality of Americans' medical information. Meanwhile, the law's emphasis on digitizing medical records, touted as a way to boost efficiency and cut costs, comes amid intensifying concerns over the security of computer networks.

Edward Snowden, the former National Security Agency contractor who has disclosed the agency's activities to the media, says the NSA has cracked the encryption used to protect the medical records of millions of Americans.

Thieves have used stolen medical information for all sorts of nefarious reasons, according to information collected by World Privacy Forum, a research group that seeks to educate consumers about privacy risks. For example:

A Massachusetts psychiatrist created false diagnoses of drug addiction and severe depression for people who were not his patients in order to submit medical insurance claims for psychiatric sessions that never occurred. One man discovered the false diagnoses when he applied for a job. He hadn't even been a patient.

An identity thief in Missouri used the information of actual people to create false driver's licenses in their names. Using one of them, she was able to enter a regional health center, obtain the health records of a woman she was impersonating, and leave with a prescription in the woman's name.

An Ohio woman working in a dental office gained access to protected information of Medicaid patients in order to illegally obtain prescription drugs.

A Pennsylvania man found that an imposter had used his identity at five different hospitals in order to receive more than $100,000 in treatment. At each spot, the imposter left behind a medical history in his victim's name.

A Colorado man whose Social Security number, name and address had been stolen received a bill for $44,000 for a surgery he not undergone.

Perpetrators use different methods to obtain the information, ranging from stealing laptops to hacking into computer networks, according to Sam Imandoust of the Identity Theft Resource Center. "With a click of a few buttons, you might have access to the records of 10,000 patients. Each bit of information can be sold for $10 to $20," he said.

According to HHS, the theft of a computer or other electronic device is involved in more than half of medical-related security breaches. Twenty percent of medical identity thefts result from someone gaining unauthorized access to information or passing it on without permission. Fourteen percent of breaches can be attributed to

hacking.

“We say encrypt, encrypt, encrypt,” said Rachel Seeger, a spokesman for HHS’s Office For Civil Rights, which is charged with investigating breaches of medical records in health plans, medical practices, hospitals and related institutions.

The records in a laptop that a fired employee lifted from the North County Hospital in Newport, Vt., last year had not been encrypted. The laptop contained the records of as many as 550 patients. Around the time that breach was uncovered, HHS cited the hospital for a second breach involving two employees gaining access to records without authorization. Those cases are ongoing.

Wendy Franklin, director of development and community relations at North County, said the hospital generally does encrypt its records. Franklin also noted that North County requires all of its employees to sign agreements not to disclose medical records and to undergo training in confidentiality laws and procedures. She also said the hospital has instituted an audit to track access to private health records.

But, in the end, Franklin said, the hospital largely has to rely on the honor system.

Two federal laws govern the confidentiality of medical records: the Health Insurance Portability and Accountability Act (HIPAA), originally passed in 1996, and the Health Information Technology (HITECH) Act of 2009. Together they lay out what health care providers and affiliated businesses are required to do to protect confidentiality of patients.

According to James Pyles, a Washington, D.C., lawyer who has dealt with health issues for more than 40 years, all 50 states have their own privacy laws and 46 of them require consumer notification when there is a security breach of private records.

HHS can impose a civil fine of between $100 and $50,000 for each failure of a business, institution or provider to meet privacy standards, up to a maximum of $1.5 million per year. A person who knowingly violates HIPAA faces a criminal fine of $50,000 and up to a year in prison. If the perpetrator tried to sell the information for “commercial advantage, personal gain or malicious harm,” he or she could face a $250,000 fine and up to 10 years in prison.

The HIPAA law includes exceptions that allow a provider to share medical information without a patient’s permission. A common example is when hospital business offices share information for the purpose of seeking payment. But there are also exceptions for “public health activities,” “health oversight activities,” “law enforcement purposes,” and other purposes. No wonder, Pyles said, some patients are reluctant to disclose to a medical provider that they have a sexually transmitted disease or a mental illness unless they have to.

Under the HITECH law, a medical provider, health plan or medical institution must notify patients when a breach of their medical records is discovered. HHS must also be contacted. HHS discloses breaches involving 500 or more patients.

Discovery of the breach is useful but doesn’t correct the mischief that may have happened. Although patients can have corrected information put in their files, it’s difficult to get fraudulent information removed because of the fear of medical liability.

“It’s almost impossible to clear up a medical record once medical identity theft has occurred,” said Pyles. “If someone is getting false information into your file, theirs gets laced with yours and it’s impossible to segregate what information is about you and what is about them.”

Pyles describes the status quo as “the worst of two worlds,” he said. The U.S. has “a regulated industry that is saddled with laws with so many loopholes that they don’t know what they are responsible for, and a public that doesn’t believe their health information is being protected.”

———

Visit Stateline.org at www.stateline.org

Distributed by MCT Information Services

———

ARCHIVE ILLUSTRATION on MCT Direct (from MCT Illustration Bank, 202-383-6064): 20071129 Internet safety

———

Topics:

t000002827,t000185378,t000412858,t000002458,t000027866,t000170636,t000002537,t000023148,t000023139,t000003813,t000