Why Thieves Want to Steal Your Medical Records

- **Megan Elliott**
- MORE ARTICLES

- March 29, 2015

Source: Thinkstock

In February, health insurer Anthem announced that a massive data breach may have exposed the personal information of millions of its customers, including their Social Security numbers, email and mailing addresses, and birthdays. A few weeks later another insurer, Premera Blue Cross, announced that it too had fallen victim to hackers. Eleven million people may have been affected.

The Anthem and Premera hacks are just the latest examples of the growing problem of medical identity theft, which involves someone stealing personal information in order to receive medical care, buy drugs, or submit fake claims. Stolen information may also be used to open new credit accounts, claim government benefits, or get a job.

From 2013 to 2014, the number of people affected by medical ID theft grew 22%, according to research by the Medical Identity Fraud Alliance (MIFA). More data breaches happen in the medical and health care industry now than in other sector, including financial, education, and government, according to the Identity Theft Resource Center.

Once someone's data is stolen, it can be difficult and expensive to resolve the problem. Sixty-five percent of victims surveyed by MIFA spent more than $13,000 in attempts to fix the issues caused by the theft, though only 10% felt that the problem had been permanently solved.

Health data is a tempting target for thieves for a number of reasons. For one, it's actually more valuable than financial information. "[O]ver the past couple of years, we've identified that medical information has a higher value on the black market than credit card information," Pat Calhoun, senior vice president of network security at Intel Security, told The Atlantic.

Source: iStock

One reason medical data is coveted by thieves is because it has more lasting value than other types of information. Once the bad guys get their hands on it, it's difficult for the victim to do anything to protect themselves. While a stolen credit card can be cancelled and fraudulent charges disputed, the process for resolving medical ID theft is not as straightforward. Hospitals and insurers usually don’t have a clear process for fixing errors on someone’s health record or for helping patients cope with the other consequences of identity theft. “Unlike credit card numbers, healthcare information is nonrecoverable, and potentially lethal in the wrong hands,” Robert Hansen, the vice president of WhiteHat Security, told the Christian Science Monitor.

Another reason that hackers have set their sights on medical data is that it’s often much easier to access than financial information. Banks and other financial service providers have stepped up their online security in recent years, but many health insurers and hospitals are behind the curve.

“While the Anthem and Premera breaches certainly shed light on the situation and should be otherwise pressuring companies to escalate their efforts, those entities should have been focusing on security already,” attorney Ken Dort said in an interview with FierceHealthIT.

In some cases, the companies holding health data seem to be inviting hackers in, especially when they’re storing data unencrypted, as Anthem was doing. Unencrypted data makes things easier for companies and their employees, but that convenience comes at a price, since it’s also simpler for hackers to read and make use of the stolen data, the Wall Street Journal reported. The Health Insurance Portability and Accountability Act (HIPAA) addresses a number of patient privacy issues but doesn’t require encryption of people’s data.

Phil Walter/Getty Images

Combine a high black market value with easy access and an increasing reliance on electronic health records, and you have the perfect storm for a spike in medical identity theft. And once thieves have that information, they can do virtually anything with it. Personally identifying information like names, Social Security numbers, and dates of birth can be used to open up new credit accounts and file fake tax returns. Health insurance information can be used to purchase drugs or medical equipment, which are then resold illegally, or even to get medical care. The latter can have consequences that go far beyond the financial.

“If someone uses your health insurance to get services, you can end up getting improper care because the thief’s medical information becomes mixed with yours,” explained Eva Velasquez of the Identity Theft Resource Center in an interview with Bankrate. “If the thief uses your insurance to get access to prescription drugs, you can end up with a flag in the system that could trigger regulators or even law enforcement to track you down.” Because there’s no central repository for health data or coordinated system for resolving disputes, it can be difficult for patients to erase this false information from their files.

Hacking isn’t the only way that your medical information can be compromised. Sometimes, health care workers steal data, while in other cases, friends or family members use a person’s health insurance information to obtain fraudulent care or file fake claims, Bankrate reported. Often, a person will have no idea that their information has been stolen until a bill shows up for a treatment they never received. At that point, it's up to the victim to try to resolve the problem.

Source: Thinkstock

Both industry and government officials seem to be waking up to the vulnerability of medical data. New Jersey Governor Chris Christie recently signed a bill requiring health insurance companies to encrypt patient data. The FDA is raising concerns about medical device cybersecurity. And leading health insurers like Aetna and Kaiser Permanente have joined forces with credit reporting agency Experian and others to form MIFA, which aims to find solutions to better protect patient data.

Some experts have proposed an even more radical solution to stop identity theft: single-payer health care. “It seems like the public health or single payer model, like in the U.K., has great equity, and the motivation to share [insurance credentials] doesn't exist because everyone has that baseline access to medicine,” Larry Poneman, the founder of cybersecurity firm Poneman Institute, told Fortune. “This concept of medical identity theft is very foreign in countries that provide health insurance to their citizenry.”