Medical Identity Theft: What Is It, How to Protect Yourself, and What to Do if You're a Victim

What Is Medical Identity Theft?

A vicious new type of identity theft is on the rise: medical identity theft. It occurs when someone steals your personal information to receive free medical care, goods, and/or prescription drugs.

"Medical identity theft is dangerous because it not only has financial implications but can have life-threatening consequences," says Steven Bearak, founder and CEO at IdentityForce, a provider of identity, privacy, and credit protection for individuals, businesses, and government agencies.

If a thief's health information is mixed with your medical records, then your treatment, health insurance, payment records, and credit report may all be affected, according to the Federal Trade Commission. Medical identity theft can disrupt your life, damage your credit rating, and waste taxpayer dollars.

Medical identity theft comes in many different forms. Here are some ways thieves are profiting from your medical identity. They:

- Make fraudulent claims against your own health insurance policy or Medicare so they can receive free healthcare;
- Obtain illegal, free, or bogus treatment by assuming your identity at a hospital or clinic to obtain their own medical care free; your health insurance plan is then billed for fake or inflated treatment claims; and
- Secure prescriptions, such as addictive drugs and medical products, which they may use or sell.

Why Medical Identities Are So Valuable

Your medical records may be more valuable than your credit card number. Here's why.

- **Access.** Hospitals have relatively low security compared to banks and credit card companies, and collecting personal information is fairly simple. Another challenge to maintaining your privacy is that there is no central repository for medical records, says Bearak.
- **Data.** Medical records contain more sensitive personal information than a bank account. With names, birth dates, insurance policy numbers, diagnosis codes, and billing information, fraudsters sell the information, create fake identities, file false insurance claims, and purchase medical equipment or drugs.
- **Timing.** Most people are not regularly checking their medical records, so the fraud may not be immediately flagged. Credit card theft, on the other hand, is quicker and easier to uncover, and the compromised accounts can be cancelled.
- **Value.** Medical identities are 20 to 50 times more valuable to criminals than financial identities, according to a recent Fortune magazine article.

Who Commits the Crime?

Medical identity thieves can be found in a wide array of places, including hacking into medical databases or breaking into medical facilities. Here's who's profiting:

- ***Hackers.*** The Affordable Care Act's HealthCare.gov website was hacked last fall, and Community Health Systems had their computers hacked by Chinese identity thieves who stole personal information, exploiting the infamous Heartbleed security flaw (discovered in April 2014) that is used by as many as two-thirds of websites on the Internet, according to a recent report in USA Today.
- ***Employees.*** Doctors, nurses, and lab technicians at healthcare facilities may be at fault. They have easy access to medical information, and their knowledge of the insurance billing systems presents opportunities for a quick profit.

- ***Organized crime rings.*** "Medical identity theft is a rapidly spreading malady, often by organized crime rings," James Quiggle, spokesman for the Coalition Against Insurance Fraud, a nonprofit alliance of carriers, consumer groups, and government agencies in Washington, D.C., told BenefitsPro.com. These crime organizations can buy stolen patient information on the black market and establish fake clinics to make bogus claims against the health policies of honest consumers.

Medical Identity Theft on the Rise

Unlike the financial services industry, healthcare companies lack the necessary measures to adequately prevent medical identity theft. What could be making the problem worse is the digitization of health information. As mandated by the Affordable Care Act, most medical providers will need to meet requirements for electronic medical records by 2015. This includes the digitized records themselves as well as the exchange of information between providers, increasing the likelihood for identity theft and data breaches.

In January 2015, Anthem Inc., the country's second-biggest health insurer servicing nearly 10% of all Americans, said hackers broke into a database containing personal information for about 80 million of its customers and employees in what is likely to be the largest data breach disclosed by a healthcare company.[1]

Although Anthem is offering free credit monitoring and identity theft repair assistance to current and former customers, this breach could have long-reaching impacts for victims.

Identity theft of medical records has become big business, occurring in increasingly alarming numbers:

- More than two million Americans were victims of medical identity theft in 2014 and medical identity theft increased nearly 22% last year, according to a study released last month by the Medical Identity Fraud Alliance (MIFA) and Ponemon Institute.
- The healthcare industry accounted for 44% of all data breaches in 2013, the most, by far, of any sector of the economy, according to the Ponemon Institute's Annual Study on Patient Privacy and Data Security.
- In the past two years, more than eight million people have been affected by a breach of unsecured medical information, according to the U.S. Department of Health and Human Services.
- More than 1.8 million Americans were victims of medical identity theft in 2013, a crime that is increasing at an annual rate of 32%, making it the fastest growing type of identity theft, according to the Identity Theft Resource Center in San Diego.
- The number of health/medical data breaches leaped from 13 in 2005 to 269 in 2013, comprising 43.8% of the 614 breaches reported in 2014, according to the Identity Theft Resource Center.

What If You're a Victim

Medical identity theft can cause serious and long-lasting damage, and recovering can take years. "If your medical identity is stolen, there could be misinformation on your record, which could result in your receiving the wrong treatment, undergoing an unnecessary procedure, and other life-threatening outcomes," says Bearak. Here are some of the consequences:

- ***Physical health threat.*** Medical identity theft is a dangerous crime that could threaten not only your financial health but your life. Imagine going to the emergency room to learn that your health insurance has been cancelled or being misdiagnosed or mistreated due to inaccuracies found in your medical records. A thief's treatment history can also end up on your medical records. This could include the wrong blood type or medicine to which you're allergic.
- ***Invasion of privacy.*** Like any data breach, information from your medical records is a private matter that potentially includes sensitive personal information that you wouldn't want everyone to know.

- ***Ruined credit.*** Thieves may accumulate significant bills in your name then disappear without paying. You could then be hounded by collection agencies; turned down for loans, mortgages, and jobs; and forced to pay higher interest rates. What's more, this form of identity theft is even harder to recover from than a financial data breach. Unlike the Fair Credit Reporting Act that has a process in place to dispute information on your credit records with the credit bureaus or debtors, Bearak says, there is no such recourse for victims of medical identity theft.
- ***Legal troubles.*** According to auditing firm Lane Gorman Trubitt, a pregnant woman stole the medical identity of a mother and delivered a baby who tested positive for illegal drugs. Social workers tried to take away the real mother's four children, falsely thinking she was the addict, and she had to hire a lawyer to keep her family intact.

What's the Cost of Medical Identity Theft?

Medical identity theft doesn't just hurt the victim—it hurts all of us. Since there are no current laws specifically requiring criminal prosecution against medical identity thieves, there is no way to accurately calculate how much medical fraud costs the healthcare industry in the United States. It is suspected, however, that it is driving up health insurance premiums in many parts of the country. Estimates of annual U.S. medical fraud range from $80 billion to $230 billion. For the fiscal year ending Sept. 30, 2013, the federal government alone recovered a record $4.3 billion from people and companies that attempted to defraud healthcare programs, according to the U.S. Department of Justice and the U.S. Department of Health and Human Services. Healthcare organizations who suffer data breaches are subject to costs that average $2 million over two years, according to estimates.

What Is the Industry Doing to Combat the Problem?

The costs associated with medical identity theft may be a primary reason why the healthcare industry and related players are starting to come together to focus on prevention. However, according to Fortune, it is a daunting task. "With so many potential avenues for information to be lost, so many different institutions from which to steal data, and so many ways of perpetrating fraud at other organizations, the industry is a long way from being as impenetrable as the financial services industry."

There is some good news, though. Protections combatting medical identity theft are slowly becoming more widely known and adopted. This year a few dozen businesses—including healthcare providers such as hospitals, integrated care payer-providers such as Kaiser Permanente, insurers, credit companies, and digital security companies—formed the Medical Identity Fraud Alliance.

What You Can Do to Protect Yourself

- **Track your medical records and check for mistakes.** Remember, you have the right to see your records and have errors corrected. Wrong information not only points toward evidence of identity theft but also has implications for your treatment.
- **Read your medical and insurance statements regularly and completely.** They can show warning signs of identity theft.
- **Review your insurance benefits.** Ask your insurer for a listing of benefits paid out under your policy at least once a year.
- **Monitor where and when you provide your personal medical information** (in person, over the phone, or online). Always decide if the information is absolutely necessary before providing it.
- **Keep paper and electronic copies of your medical records and health insurance records in a safe place.** And, when no longer needed, shred documents containing personal information.
- **Look for medical organizations that follow the "Red Flags Rule,"** which requires many businesses and organizations to implement a written identity theft prevention program designed to detect the "red flags" of identity theft in their day-to-day operations and take steps to prevent the crime and mitigate its damage.

Consider Medical Identity Theft Coverage

Medical identity theft is just one way thieves can gather your personal data. Protecting yourself is paramount. Much like you insure your home and car, health and life, it is equally important to protect your personal information.

Companies like IdentityForce offer medical identity theft protection plans that includes three layers of protection, including comprehensive identity monitoring and near real-time alerts of suspicious activity, assistance with obtaining a report from insurance companies for all benefits paid to the subscriber's account, and medical identity theft insurance coverage. To learn more about how you can work with the IdentityForce team to protect yourself from the damages of medical identity theft, visit the services section or call toll-free at 1-877-IDFORCE.

Unfortunately, once you're involved in a data breach, you are at an increased risk of falling victim to identity theft. So, in addition to regularly monitoring your financial statements and credit report, you'll want to make sure you stay on top of your insurance benefits and medical records, too.

[1]Tony Bradley. "5 things all Anthem customers should do after the massive data breach," PC World. http://www.pcworld.com/article/2880611/5-things-all-anthem-customers-should-do-after-the-massive-data-breach.html (Accessed February 20, 2015); Herb Weisbaum. "Millions of children exposed to ID theft through Anthem breach," NBC News. http://www.nbcnews.com/business/personal-finance/millions-children-exposed-id-theft-through-anthem-breach-n308116 (Accessed February 20, 2015); Mark Pribish. "Security breaches a big issue for healthcare." Identity theft Center. http://www.idtheftcenter.org/Data-Breaches/security-breaches-a-big-issue-for-healthcare.html (Accessed February 20, 2015).