

Pharmacy Solutions

June 2009

1

Medical Identity Theft Turns Patients Into Victims

If identity thieves were to disregard your financial accounts and instead target your medical information, your first thought might well be, "Take my medical identity. Please." What nut would want your high cholesterol, trick knee, and family history of Alzheimer's? The answer is simple: someone without health insurance who needs surgery or prescription drugs, or someone who sees a medical ID as the open sesame that will allow him or her to collect millions in false medical claims. These thieves don't actually want your medical ailments, of course, but by pretending to be you they can get what they're really after.

Untangling the mess is hard: Unlike financial identity theft, there's no straightforward process for challenging false medical claims or correcting inaccurate medical records. For victims, the result can be thousands in unpaid charges, damaged credit, and bogus, possibly dangerous details cluttering up their medical records for years to come.

The last time federal data on the crime was collected, for a 2007 report, more than 250,000 Americans a year were victims of medical identity theft. That number has almost certainly increased since then, because of the increased use of electronic medical records systems built without extensive safeguards. As the push toward electronic medical records gains momentum, privacy experts worry those numbers may grow substantially. They're concerned that as doctors and hospitals switch from paper records to EMRs, as they're called, it may become easier for people to gain unauthorized access to sensitive patient information on a large scale. Consumers may not even know their records have been compromised.

In January 2008, a new law took effect in California that requires providers to let consumers know if their medical information has been "breached." But only a handful of other states spell out notification requirements regarding unauthorized release of patient medical data. In contrast, most states have so-called breach laws that address accidental disclosures of financial information; these may also apply to medical data in certain instances.

Victims of financial identity theft have a much clearer path to recovery than those whose medical identities are stolen. If someone swipes your wallet and goes on a spending spree, you can ask any of the three major credit bureaus for a free credit report, place a fraud alert on your account, and get inaccurate charges expunged. With medical identity theft, it's not that



simple. In the first place, your records are most likely scattered among many different providers, and there's no medical records clearinghouse that keeps them.

Under HIPAA, the federal law that addresses medical privacy, you're entitled to a copy of these documents, though you may have to pay for it. If there's an error, you can add a correction to the record, but you can't have information deleted. And if an impostor gets healthcare services in your name, you may really be stuck. Healthcare providers may actually refuse to let you see your own record because once it's intermingled with someone else's, that person's privacy must be protected.

Even seemingly obvious errors can be hard to clear up in this fragmented system. Wayne Ivey, who formerly led an identity theft task force at the Florida Department of Law Enforcement, remembers getting a call from an extremely agitated Illinois woman a few years ago. A hospital in Miami, she said, was calling her repeatedly and demanding that she pay a \$2,000 bill for giving birth. She told the callers she'd never been to that hospital—and was 72 years old. It still took weeks of phone calls to various agencies to resolve the problem.

Feedback is always welcome!

Ginger Campbell, Pharmacy Benefit Consultant

225-336-5304 or pharmacy@bxsi.com

Until recently, experts believed most medical identity thieves were solo operators who pretended to be someone else because they needed medical care. Now a different picture is emerging, one of employees inside the healthcare system



stealing patients' information to make false insurance claims. "It's trending above the 90th percentile that insiders are doing the identity theft," says Pam Dixon, executive director of the World Privacy Forum, who authored a 2006 report on medical identity theft that was perhaps the first in-depth examination of this crime.

An insider was behind the theft of more than 1,100 Medicare beneficiaries' medical identities at the Cleveland Clinic in Weston, Fla., a few years ago. A front desk clerk named Isis Machado downloaded their names, addresses, and Social Security and Medicare numbers and sold the data to her cousin, who then made more than \$2.8 million in false Medicare claims. Machado was caught because a coworker told her supervisor she was acting suspiciously. "There's no way to prevent insiders from becoming crooks," says Robert Gellman, a privacy and information policy consultant in Washington, D.C. With sometimes hundreds of employees legitimately needing access to patient records, even robust computer monitoring and auditing systems may not pick up a problem.

Healthcare providers can be victims, too. A dying man confessed to his doctor that he'd posed as a cousin to fraudulently receive more than \$85,000 in medical services at the University of Connecticut Health Center in Farmington. The hospital got stuck with the bill when the patient died. It now requires a picture ID at every visit and pastes a photograph to the inside of each patient's medical chart, says Marie Whalen, assistant vice president for ambulatory services. But that's not going to protect the facility from the kind of insider crime that experts now believe is more common.

In addition, the health plan may maintain the inaccurate information in its database and may share the information with the MIB Group, Inc. This corporation, owned by insurance companies, maintains a database for members to exchange confidential information about individuals



who apply for health and other types of insurance benefits. Additionally, until such time as all third-party payer

records are corrected, victims could be denied payment for health services rendered or be denied additional health, disability, or life insurance coverage should it be sought. Healthcare providers and health plans may suffer permanent damage to their reputations, which may result in irreversible business consequences.

The impact of medical identity theft on society is significant as well. Private-pay patients may find themselves paying more to healthcare providers to offset write-offs for medical identity theft. Purchasers of insurance may see increased rates to offset losses insurance companies may incur. Tax payers may pay additional taxes for government-provided benefits to offset the cost of undiscovered or unrecovered claims. Tax payers also pay for increased federal and state law enforcement services to cover investigation, prosecution, incarceration, and enforcement with regard to medical identity theft. Tax payers might even be subsidizing drug-seeking behaviors when the stolen identification is used to obtain narcotics and pain-killers under false pretenses.

Ultimately, no matter how sophisticated the technology or diligent the healthcare provider, patients themselves may be the best first line of defense against medical identity theft. "Most of the time, these problems are consumer reported," says Byron Hollis, managing director of the national antifraud department for the Blue Cross Blue Shield Association, which coordinates antifraud activities for the 39 independent BCBS companies nationwide. "They know what procedures they did or didn't receive."

Preventing and Detecting Medical Identity Theft

The prevention and detection of medical identity theft requires diligent monitoring and appropriate response. Responses may include a variety of administrative, technical, or physical safeguards. HIM (health information management) professionals (as well as privacy and security officers and other organizational leaders), individuals, healthcare organizations, health plans, and other stakeholders who may be affected must work in cooperation to establish prevention and detection programs.



Feedback is always welcome!

Ginger Campbell, Pharmacy Benefit Consultant

225-336-5304 or pharmacy@bxsi.com

The first line of defense may well rest with the individual. Individuals are encouraged to practice the same preventive measures for medical identity theft as they would for financial identity theft. Common preventive measures include:

- Sharing personal and health insurance information only with trusted providers.
- Monitoring the explanation of benefits received from insurers and obtaining a summary each year of all the benefits paid in the patient's or guarantor's name.
- Contacting the insurer and provider about charges for care that was not received, even when there is no money owed.
- Maintaining copies of healthcare records.
- Checking personal credit history for medical liens.
- Demanding that providers and insurance companies correct errors or append and amend medical records to alert a user to inappropriate content.
- Questioning "free" medical services or treatments (sometimes illicit entities use the lure of "free" services to obtain names and insurance information for use in fraudulent claim submissions). Individuals should always question what is being offered and who is paying the cost. If not satisfied with the answers, they should decline the offer.
- Protecting health insurance information. Individuals should safeguard insurance cards, explanation of benefits, and health plan correspondence in the same way they would safeguard credit cards.
- Refusing to provide insurance numbers to telephone marketers or door-to-door solicitors

Feedback is always welcome!

Ginger Campbell, Pharmacy Benefit Consultant
225-336-5304 or pharmacy@bxsi.com

Healthcare Fraud Quiz

Are you at risk? Test your knowledge!

1. **Healthcare fraud accounts for up to \$100 million in losses annually.**
A. True B. False
2. **Intentionally giving false information on a claim is not fraud if a service, any service, was performed.**
A. True B. False
3. **An accident purposely committed in order to receive benefits of any coverage is healthcare fraud.**
A. True B. False
4. **A person who intentionally sends a forged or altered document through the U.S. mail or fax machine has committed a crime.**
A. True B. False
5. **The term "clean sheeting" means obtaining life insurance policies by hiding life threatening illnesses.**
A. True B. False
6. **An application for coverage purposely signed and dated to conceal an illness or injury in order to receive coverage can be considered a fraudulent application.**
A. True B. False
7. **A material misrepresentation occurs when an important fact is omitted from a document.**
A. True B. False

Quiz Answers: 1.B (losses in billions), 2.B (intentionally giving any false information for any reason is fraud), 3.A, 4.A, 5.A, 6.A, 7.B (it must be intentionally omitted to be considered fraud), 8. A.