

Medical Identity Theft Turns Patients Into Victims

By *Michelle Andrews*

Posted February 29, 2008

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: one 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.



Medical identity theft currently accounts for just 3 percent of identity theft crimes, or 249,000 of the estimated 8.3 million people who had their identities lifted in 2005, according to the Federal Trade Commission. But 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. In addition, Microsoft, Revolution Health, and, just this week, Google have announced they're developing services that will allow consumers to [store their health information online](#). Consumers may not even know their records have been compromised. In January, 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

People Who Read This Also Read

- [What to Do When Thieves Snatch Your Medical Identity](#)
- [Saving on Surgery by Going Abroad](#)
- [Electronic Medical Records: Will Your Privacy Be Safe?](#)
- [Medicine Methodology](#)

How an Electronic Medical Record Can Help Keep Your Family Healthy

Recommendations by **loomia**

of financial information; these may also apply to medical data in certain instances. This month, Democratic Reps. Ed Markey of Massachusetts and Rahm Emanuel of Illinois, with support from several privacy groups and Microsoft, introduced a bill that would strengthen safeguards protecting access to consumers' medical information and make it a federal requirement to notify patients if their healthcare data get exposed.

Brandon Reagin didn't realize someone had snatched his medical identity until his mother called to tell him he was the lead suspect in a car theft in South Carolina in 2005. The 22-year-old marine had lost his wallet more than a year earlier while celebrating with friends after completing boot camp at Parris Island, near Beaufort, S.C. After his training, he was posted to California. But in South Carolina, Reagin lived on, as an impostor used his military ID and driver's license to not only test-drive new cars and then steal them but also visit hospitals on several occasions to treat kidney stones and an injured hand, running up nearly \$20,000 in medical charges. Reagin found out about the unpaid hospital bills when he asked for a credit report following the car theft. "It was horrible," he says. "And what made it worse is that no one really knew what to do when it first started happening."

Reagin got nowhere with local police, but with the help of a state senator, he finally connected with the U.S. attorney's office in South Carolina. Staff there notified the Secret Service, and Reagin's doppelgänger, a 30-something guy named Arthur Watts from a tiny Midlands town called Blythewood, was eventually arrested. Watts pleaded guilty last September to identity theft and is awaiting sentencing.

But for Reagin, now serving in Iraq, the case isn't closed. Because of the outstanding hospital bills, the state intercepted his \$362 tax refund, money he has yet to see. And although the hospitals no longer dun him for the unpaid balances, he's still trying to clean up his credit. (In addition to racking up medical bills, Watts opened cellphone and other accounts in Reagin's name and stole another car.) There's another potential problem: The hospitals Watts used may have medical records in Reagin's name for treatment he never received. If he visits his family in South Carolina and needs medical attention, those records could complicate his treatment, even cause harm. And if those medical records someday become electronically linked to one big nationwide health information network, as envisioned by the Bush administration, some privacy experts worry it may be impossible to find and correct the errors once they percolate through the vast interconnected system. Others argue that the technology could actually make tracking errors easier. The reality is unclear.

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.

Insider fraud. 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.

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."

Tags: [medical safety](#) | [medical records](#) | [identity theft](#)