

The impostor in the ER

Medical identity theft can leave you with hazardous errors in health records

By Richard Rys

Self

updated 7:38 a.m. CT, Thurs., March. 13, 2008

Katrina Brooke felt well prepared for the birth of her son, Andrew, three Aprils ago. The only complication was her Caesarean section; otherwise, everything went smoothly. After three days in the hospital, Brooke returned to her home outside of Seattle to recover and enjoy her baby boy.

Three weeks later, as Brooke stood in her kitchen opening mail, she found a curious \$94 bill from a local health clinic, a place neither she nor her husband had ever heard of. Stranger still, the notice was addressed to her newborn son: Andrew had apparently visited the clinic and been prescribed the painkiller OxyContin for a work-related back injury.

It seemed like a simple clerical error at first — one that might even have been funny, considering the only labor Andrew had been involved in was his own birth. But the more Brooke scrutinized the letter, the more concerned she grew. Andrew's middle name was on the bill, and no one knew the baby's full name but a handful of friends and family — as well as the hospital, where she had filed the paperwork for Andrew's birth certificate, which included their family's home address and Social Security numbers and Brooke's maiden name.

A call to the clinic confirmed that a mystery man had used their child's newly minted identity to obtain health care only one week after Andrew was born. The Brookes had become victims of a crime they'd never heard of: medical identity theft. "People aren't aware of this unless it happens to them," Brooke says. "When you first get the bill, you're confused. Then when you delve into it, you think, What other information do they have? What else is going to happen to us now? At that point, it was scary."

Luckily for the Brookes, the clinic agreed to waive its charges. But for many victims, the crime doesn't surface until unthinkable damage has been done. The worst case: insurance maxed out to its lifetime limit, years spent untangling paper trails, and medical records permanently altered. Unlike a stolen credit card or savings account number, this kind of identity theft could be life-threatening. Imagine what could happen if someone else's medical history was injected into your records: You could arrive at an ER and be given the wrong type of blood or be refused medication because your file says you are allergic. And because mistakes in medical records can be notoriously hard to expunge, you could spend years convincing doctors you weren't actually diagnosed with the diseases, mental illness or substance-abuse problems appearing in your file.

According to a recent survey by the Federal Trade Commission (FTC), 3 percent of U.S. identity-crime victims had someone use their personal information — a Social Security number, an insurance policy ID, even a mere driver's license — to obtain medical services or to profit from filing false claims in their name. That means nearly 250,000 Americans may be victims each year. For an increasing number of career criminals, health care workers and consumers struggling to keep up with bills, the lure of medical identity theft is too great to resist, notes Chris Dorn, a fraud expert with Ingenix, a health care fraud investigation firm in Eden Prairie, Minnesota. "The overall cost of health care has risen so much that it has become a valuable commodity," Dorn says. "Any time you have 47 million Americans without adequate health care coverage, you will have people out there willing to steal it."

The stakes are high

It took one phone call to make Anndorie Sachs, a mother of four in Salt Lake City, aware of how serious medical identity theft has become. She says that in April 2006, a Utah social worker notified her that her newborn had tested positive for methamphetamines — as a result, the state planned to take away all of her children. In fact Sachs, then 27, hadn't been pregnant in more than two years; her stolen driver's license had ended up in the hands of Dorothy Bell Moran, a meth user who gave birth using Sachs's name. After a tense few days of phone calls with child services, Sachs was allowed to keep her kids. She then hired a lawyer to sort out the damage to her legal and medical records, and figured her worries were over.

Months later, when Sachs suffered a kidney infection, she was careful to avoid the hospital where Moran had used her identity. It didn't matter: The thief's records had circulated electronically and intermingled with her own. Moran's emergency contact number was listed in Sachs's file, and there may have been other mistakes, such as the thief's blood type. Sachs — who has a blood-clotting disorder and for whom the wrong medication could be disastrous — was savvy enough to alert the hospital staff, who straightened out her charts before making a critical error. "Had [Moran's] baby not tested positive for drugs, I wouldn't have known anything about it," Sachs says. "I have a hard time believing that everything is back the way it was before. It's terrifying to think about."

Consider the number of people who see your personal information when you become sick. "There are so many players," says Robert Gellman, a privacy consultant and attorney in Washington, D.C. "Doctors, hospitals, pharmacies, labs, insurance companies — any single medical treatment can involve a half dozen entities." To turn your life upside down, it takes only one person at one of those places willing to use her access as an opportunity for exploitation. In Florida, an office coordinator at the Cleveland Clinic in Weston printed out 1,100 patient records, then sold them to her cousin for \$5 to \$10 per patient, according to an FBI agent involved in the case. The World Privacy Forum, a nonprofit research group in San Diego, reports that prosecutors in New York, California and Florida have uncovered a technique that would make Tony Soprano proud: "clinic takeovers," in which criminals buy a health care center, steal information from it to file false insurance claims, and then shut the whole thing down before anyone catches on.

It's not just professional crooks working the system. In Miami, physicians sold their medical licenses and provider numbers to a clinic that racked up \$6.5 million in false claims. A Boston-area psychiatrist altered records of his patients and their families to reflect sessions and diagnoses they didn't have, then billed insurance companies for treatment he never provided. Then there are victims like Joanne Lomax of Philadelphia, a 32-year-old package handler who was surprised when her insurance rejected her claim for a \$189 gynecological visit. She was even more stunned to learn why — only one annual checkup was covered, and another woman had already used Lomax's name to pay for her own exam.

As Lomax learned, your insurance card isn't just something you dust off for doctor's appointments — in the hands of a thief, it becomes a credit card, a PIN and a license to spend. FTC numbers suggest that medical identity crimes may cost the U.S. economy \$468 million per year. "This crime is so insidious," warns Pam Dixon, founder and executive director of the World Privacy Forum. "It affects more people than you realize — and the stakes are as high as they can get."

Regaining control of identity

On Christmas Day in 2003, Jo-Ann Davis pulled out of a gas station near Pittsburgh without realizing she'd left her wallet on the roof of her car. She hoped she could minimize the damage by quickly canceling her credit cards. But her

insurance card was in the wallet, too. Before her identity thief was caught, she had used Davis's information nearly 40 times, racking up almost \$14,000 in prescription meds and treatment in Pennsylvania and Ohio.

For the next four months, regaining control of her identity became a second job for Davis, a 42-year-old veterinary nurse. She exchanged faxes and phone calls with her insurer and fended off bill collectors. She says the police investigated her to make sure she wasn't a conspirator. And then came the day she stopped by her pharmacy to pick up her migraine medication. When a well-meaning clerk noticed her account was flagged and called the police, Davis was nearly arrested. "I don't think my insurance company realized the magnitude of this," says Davis, who eventually convinced the cops she wasn't her impostor. "You don't know how long this is going to go on."

The unsettling reality is that it's far easier to safeguard your financial well-being than records that could affect your physical health. "On the medical side, we're at the same stage as we were 10 years ago with financial identity theft," Gellman says. Three credit bureaus serve as centralized gatekeepers to your financial records; it takes mere minutes to download a free annual credit report. It could take years to track down the hundreds of records compiled by every medical provider you've ever used. And after you've found them, some providers charge hundreds of dollars to copy all the pages.

Complicating matters is the federal regulation designed to protect your medical privacy — the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. In theory, the rule provides access to your medical records and the ability to correct mistakes. But in practice, when patients challenge the accuracy of their files, insurance companies and physicians are often loath to delete information, preferring to red-flag the items in question. No one is compelled to amend records they didn't create, so if an M.D. submitted a claim to your insurance based on an identity thief's scam, the insurer is not required to correct it as long as the doctor is still in business. "There's a tendency among medical professionals to be suspicious of why you need to make changes," says Adam Levin, chairman of Identity Theft 911, a crisis-resolution firm in Scottsdale, Arizona.

Worse yet, once someone else's history is entangled with yours, health care providers will sometimes prevent you from seeing that information, for fear of violating the thief's privacy rights under HIPAA. When Sachs asked to see her records at the hospital where the impostor had given birth under her name, officials refused, saying the records were no longer technically hers. "The hospital said they're not the police — they're in the business of trusting people," she recalls.

'You have to be persistent'

The costly, time-consuming investigation of these crimes often falls on the victim's shoulders. "To say there's little recourse for these folks would be an understatement," Dixon says. Brooke and her husband had to go to two stations before police agreed to look into the matter; at the time in Washington, some medical ID theft was treated as a property crime, akin to a stolen iPod or car break-in on the police priority scale. On the federal level, the FTC logs complaints but doesn't have the authority to pursue them. The U.S. Department of Health and Human Services is the agency to contact if you're denied access to your medical records. Although every insurance company has its own investigators, victims may be made to feel they aren't a priority, says Byron Hollis, managing director of the Blue Cross and Blue Shield Association's national antifraud department in Washington, D.C. "There are a lot of different kinds of fraud, and medical ID theft is a small subsection of that. So the consumer may feel, when they first call, that it's the most important thing to them, but the person they're talking to may have 20 to 40 cases of other kinds of fraud they're working on. You have to be persistent."

Thirty-nine states have laws requiring companies to alert you when a security breach compromises your personal information, but not all of the laws specifically protect medical information. A California law that took effect in January took that step, and other states may follow. But lawmakers have made little headway on fixing federal laws so that they affirm the victim's right to clear corrupted medical records. Meanwhile, there's an Orwellian scenario keeping privacy advocates up at night: The government is moving forward with plans to create an online records locator called the Nationwide Health Information Network, designed to help physicians share records. Its upside is that doctors would have nearly instantaneous access to your health history in an emergency, no matter where you are. On the other hand, millions of health care workers — and potential criminals — could be a mouse-click away from those same records.

With so little standing between your health information and the con artists who covet it, the future of medical identity theft might get worse before it gets better. But as more victims step forward, more legislators will be pressured to take action. In Washington, the story of the Brookes and their son, who may be the youngest identity-theft victim in the country, helped inspire a measure now making identity theft a priority for law enforcement across the state. Two-year-old Andrew was sitting on the lap of Governor Christine Gregoire as she signed the law. "At least one good thing came out of it," Brooke says. "When you're affected by this crime, you want to see things change. I'd like to see other states pass similar laws. This is just the beginning."

Copyright © 2007 CondéNet. All rights reserved.

URL: <http://www.msnbc.msn.com/id/23392229/>

[MSN Privacy](#) . [Legal](#)

© 2008 MSNBC.com