

## **Medical Identity Theft: The Aftermath**

### **Three years later, a medical identity theft victim finds prevention isn't up to snuff.**

Three years later, a medical identity theft victim finds prevention isn't up to snuff.

By Cheryl McEvoy

Last February, *ADVANCE* shared the [story](#) of Anndorie Sachs, a mother of four who was the victim of medical identity theft. Now nearly 3 years after the incident, Sachs is still untangling the mess of medical records and doctor bills left behind. She shared some of the lessons she's learned over the years and what hospitals should be doing to reduce the threat of theft.

#### **A Hidden Crime**

When Sachs realized her driver's license had been stolen, she alerted the usual authorities: she called the police and contacted credit monitors. But the local hospitals never crossed her mind. It wasn't until she was accused of giving birth to a baby under the influence of drugs that she learned her identity could be hijacked for health care.

"I'd never even heard of medical identity theft," Sachs said. "I didn't consider it as something that could even be done."

Identity theft is a highly publicized crime in the financial sector, but until recently, the illegal use of another's identity to access health care has generated little hubbub among the public. Lack of public awareness has also left victims to their own devices when responding to medical identity theft.

"It was my fault basically," Sachs recalled. "It was my job, my mess, my stuff. That's really what irritates me--that the laws aren't there."

#### **Setting the Record Straight**

Sachs managed to clear her medical records of false data, but the clean-up process took months of endless phone calls and records requests. The identity thief posed as Sachs at two hospitals, and each responded differently to the identity theft. One hospital cooperated with Sachs during the recovery process, but the other seemed to erase any record of Sachs' case. "I don't know if they shuffled my record somewhere else; I don't know what they did," she said.

Now when Sachs calls to discuss a lingering doctor's bill, the hospital claims the billing number doesn't exist. "I called a couple of times and have such a hard time getting anywhere with them," she said.

Bill collectors are still hunting her down.

While her own record has been cleared, Sachs is more concerned about the baby's medical records—a problem she didn't think of until a lawyer brought it to her attention. Originally, all of the documents noting the baby's birth referred to Sachs as the legal mother. Sachs' lawyer cautioned that if the documents weren't changed, Sachs could be held responsible for the child's welfare, including child support payments. With the lawyer's help, Sachs amended the documents and is now referred to as the "misidentified mother."

Sachs still worries she is named in the baby's other records, which she cannot access due to HIPAA protections. "The one thing I wonder about and I don't know I'll ever know for sure is if my name is scattered throughout the record of the child," she said.

As soon as Sachs learned a baby was involved, she informed the hospital that it was not hers. But months after the birth, she still received calls about the child's doctor appointments and test results.

#### **Fool Me Twice**

Sachs said the most frustrating part of recovery was the lack of support from hospitals. As she was cleaning up her records, she was shocked to learn one of the hospitals involved in her case reported a similar incident 3 years before Sachs was victimized. In the earlier case, a woman gave birth to a baby under another woman's name. "The woman who had her identity stolen ended up with the bills and the birth certificate in her name," Sachs said. "They never caught the mom or the baby. They just left the hospital."

Despite the alarming crime, the hospital didn't take any measurable steps to advise Sachs when her identity was stolen. Nor do they seem eager to develop better security measures after the second incident, according to Sachs. She believes the lackadaisical attitude is all too common.

"It still surprises me that the laws aren't stricter and there's not more being done by the hospitals to prevent it. I really think it's not being taken as seriously as it needs to be taken," she said.

### **The Red Flag Rule**

Noting a lack of identification protocol, the Federal Trade Commission passed the Red Flags Rule requiring hospitals to develop written procedures for preventing and monitoring identity threats. Each facility must identify certain "red flags" or indicators that will alert staff to a potential identity theft, whether the threat is in-house or external. The rule will take effect on May 1, so many hospitals are scrambling now to have measures sorted out by the deadline.

Sachs questions how effective the red flags will prove to be. It's better than nothing, she said, but "I don't think the red flag system will work that well."

In her case, the thief used Sachs' driver's license, which includes an identifying photo. Sachs said she and the woman didn't look alike, but the woman still managed to register under her false identity. Sachs doubts a red flag program based on photo identification would do much to halt thieves.

"Through my experience it still seems like [identity protection is] pretty disorganized," Sachs said. "I don't know that there was any way I could have prevented it from happening to me, other than to just keep my identity safer in the first place."

### **Giving Security a Hand**

Keeping identifying information under lock-and-key may be an impossible dream, but Sachs noted one type of emerging technology that shows promise. Biometric technology is gaining ground in financial and health care institutions as a way to verify identities through an optical, fingerprint or vein scan. The scan is more secure than traditional photo identification, and once a patient is registered, the chance of identity theft is virtually eliminated because no other individual can produce an identical scan.

BayCare Health System in Tampa Bay, FL, introduced PatientSecure's vein scanner from HT Systems, Tampa, FL, last May as a tool to speed patient registration and comply with the impending Red Flags Rule. According to executives, the health system selected a vein scanner because it was more reliable than fingerprint scans, which can be altered by cuts and age, and is less invasive than optical scans.

During the vein scan, the patient's hand rests about 3 inches above the scanner while a near infrared camera produces a patterned image. Each pattern is tagged with the patient's identity. If a hospital is electronic, the identifying pattern can also be linked to the patient's EHR, so the doctor can find out allergies and medications with a simple scan of the patient's hand.

"The response from our patients has been extremely positive," BayCare executives told *ADVANCE*. "There's been a lot of buzz about the new technology in the community as well."

BayCare has registered more than 70,000 patients with PatientSecure, and the system also has found success at health systems in North Carolina and California.

Sachs has seen the vein scanner in action and hopes to convince local hospitals to consider the technology. "I'm just a huge fan of what PatientSecure is doing, and if hospitals caught on to that it could make a big difference," Sachs said.

The scans improve security, but can only do so much. Unresponsive patients who are not already in the system and those who refuse vein scans must be registered the traditional way, leaving a potential loophole for identity theft. Hospital vigilance, therefore, must be the ultimate defense. "It's going to get to be a bigger and bigger problem until it's listened to," Sachs said. "Fix things now and hopefully more people won't have to go through this before it gets resolved."

For more information on BayCare's use of PatientSecure vein scans, read "[Security of Patient IDs](#)" from *ADVANCE for Health Information Executives*.

*Cheryl McEvoy is an editorial assistant with ADVANCE.*