



Stop, Thief

How to protect yourself against medical identity theft.

BY KIMBERLEE ROTH

You've probably heard them before, those (good) tips to prevent having your identity stolen: Shred documents containing credit card numbers and don't give your social security number to anyone over the phone, for starters. But few consumers are aware of how to protect themselves against a growing and disturbing trend: medical identity theft.

Medical identity theft is the fraudulent use of another person's medical identity in order to obtain medical services and medications or to bill a third-party payor such as an insurance company or Medicare. Thieves may steal a social security, health system ID, driver's license, or health insurance policy number as well as other personal information in order to pose as someone else.

The crime can have long-lasting and dangerous effects, both on your health and your finances. The thief may obtain health services in your name or bill fraudulently for services that, although you never received them, could max out your annual or lifetime insurance limits. Whether the thief is actually receiving medical treatment or just billing for fictitious treatments in your name, incorrect information—about blood type, diagnoses, or drug allergies, for instance—may infiltrate your medical records as a result. Unpaid bills listing you as the patient may be sent to debt collection agencies and reported under your social security number to credit bureaus, affecting your credit history.

A recent survey done by the Ponemon Institute, a consultancy that conducts privacy and data security research, estimates that about 1.85 million people will be affected in 2012, up from 1.49 million in 2011.

The incidence is indeed growing—at a rate of between 3 and 7 percent annually,

says Pam Dixon, executive director of the World Privacy Forum (WPF), a nonprofit that conducts research and consumer education on privacy. "And there's a striking pattern in terms of geography," she says: Although the crime occurs throughout the country, medical identity theft tends to be more prevalent in areas such as Los Angeles, Phoenix, South Florida, and New York. The patterns correspond to an aging population and the presence of Medicare and Medicaid processing centers, according to Dixon. "When you get more health care, you're more prone to be a victim of medical identity theft," she says.

That said, anyone can have their medi-



A GROWING PROBLEM Map from World Privacy Forum shows location of medical ID theft complaints collected in 2008–2009 by the Federal Trade Commission.

cal identity stolen, whether you have private insurance, Medicare, or Medicaid. "Medical identity theft is a large national fraud trend that can bite almost anyone who's not alert to the possible schemes," says James Quiggle, director of communications for the Coalition Against Insurance Fraud.

Perpetrators may belong to organized crime rings; others are individuals who need medical treatment and steal identities to avoid paying for care, says Quiggle, adding that it's common for the thief to know the victim.

The crime can skirt detection for a long

time. "People often find out years after the fact—two, five, even 10 years after," says WPF's Dixon.

According to the recent Ponemon Institute survey, collection (dunning) letters—for an unfamiliar doctor visit or procedure, perhaps—are the most common clues to victims of the crime. Mistakes in medical records such as the wrong blood type or diagnosis and suspicious entries on statements or invoices also are common.

PROTECTION IS THE BEST MEDICINE

Since anyone can be victimized and detection often takes time, a proactive stance is critical, especially for people with chronic illnesses.

Dixon is adamant: "The first and most important thing patients should do is get a copy of their medical records now. That way, if something is changed [later] without your knowledge or permission, you can prove you are who you say; you can prove your medical history."

Dixon recommends compiling a clean "snapshot" of your medical records once a year. You should be able to review these files at no charge; then, you can select only the most important information to be duplicated, such as summary sheets or hospital discharge notes, in order to avoid spending too much money.

What you're after, says Dixon, is "a good baseline of information" about your health. That could mean information such as blood type, medical conditions, surgeries, and prescription drugs you take.

There's no one-size-fits-all checklist of what to obtain since each patient's situation and medical history are unique. Bottom line, "You want enough information to reconstruct your healthcare history in case your records get corrupted or polluted in some way," Dixon says.

She recommends the following:

- ▶ Request key information about your health status and conditions from your primary care doctor and the specialists you see. If you've had surgery, obtain records about procedure(s) undergone from the hospital, too. (Dixon sees less benefit to getting copies of lab work.)
- ▶ If you've had imaging tests, request one or two representative images.
- ▶ From your pharmacy, request a record of all the prescriptions you've had filled.
- ▶ On an annual basis, call your insurer and confirm your address, then request a list of the benefits paid on your behalf over the past year. Review it carefully for misinformation. In case of a crime, "you'll typically see huge dollar amounts—like a surgery for \$200,000—or high volumes, such as 60 breathing treatments. It's usually something dramatic," says Dixon.

Other steps you routinely can take to protect yourself include:

- ▶ Treat your insurance identity information as if it were a credit card account number. Be cautious at special events such as health fairs, which can be staged, and of phone solicitations. Avoid offers of free services and services for which the "provider" will waive your copayment, recommends Calvin Sneed, director of anti-fraud programs for Blue Cross Blue Shield Association (BCBSA). Never sign a blank insurance form.
- ▶ Don't let explanation-of-benefit statements from your insurer sit in a pile of unopened mail. Review them like you would a restaurant bill or grocery receipt. If you see an unfamiliar procedure, doctor name, or service date, call to inquire.
- ▶ Be observant at your doctor's office. Are other patients' records visible to you at

"The most important thing patients should do is **get a copy** of their medical records now."

the registration desk? Do employees get up from their computers while confidential information is displayed? "As patients, I think we have to hold our providers accountable," says David Evans, M.B.A., who chairs the Business and Research Administrators in Neurology Society (BRAINS) office manager group at the American Academy of Neurology. Evans also is chief operating officer at Texas Neurology, a private practice in Dallas. "Don't be afraid to ask your doctor or the front office how they handle your information."

Under the *Health Insurance Portability and Accountability Act* (HIPAA), patients have the right to review and potentially amend their medical records. The WPF has a detailed patient guide to HIPAA on its website. (For more *Neurology Now* stories on HIPAA and obtaining medical records, go to bit.ly/ieQjxy and bit.ly/c7eLC9.)

- ▶ Listen carefully. It's easy to tune out what may seem like the umpteenth round of questions from medical assistants, nurses, and doctors, but they can tip you off to a problem: "I see here that you have MS" (you don't) or "So how is that new medicine working for you?" (What new medicine?).

THE ROAD TO RECOVERY

If you learn your medical identity has been stolen, tap your reserves of patience and persistence. Resolving the financial effects and correcting your records won't happen overnight. "It usually takes about two years," says Dixon.

If a debt collector is pursuing you, contact the healthcare facility that's billing for

the fraudulent services. "Don't pay a cent on a debt that doesn't belong to you or you will own it," Dixon adds.

You'll need to get in touch with your insurer, too, whether public or private. Sneed of BCBSA recommends calling both the customer service number and the anti-fraud department to report the theft.

Victims should file a police report at their local precinct. The police may or may not investigate, but the report becomes part of the paper trail to help you resurrect your records and credit.

Contact one of the three credit reporting agencies: Equifax, Experian, or TransUnion. Place a 90-day fraud alert on your account, and request that the other two bureaus do the same. Once you have a police report and other evidence, you can extend the alert for seven years.

You also can notify the Federal Trade Commission at **1-877-ID-THEFT (438-4338)** or **1-866-653-4261 (TTY)** as well as the FBI and your state attorney general.

Work with your healthcare provider, hospital, and insurer to correct your medical records. This is where your clean baseline snapshot comes into play, helping you prove you didn't have that \$200,000 surgery or those 60 breathing treatments. Even so, some entities may refuse to amend your medical records. In this case, you still have the right to place a statement in your file saying you disagree, and why.

If your case is complex or you're repeatedly victimized, you might consider hiring an attorney. A local bar association or legal aid society should be able to provide referrals.

Perhaps most importantly, document your communications with all parties—and know that there is a bright spot. "Now we know it's happening, and victims are getting a lot more support," Dixon says. "In 2005, no one was aware of the victim's side. We're making headway." NN