

How to protect yourself from medical identity fraud. A first step: Don't tweet health issues.

By: Christie Aschwanden, The Washington Post

Most of us tightly guard our credit cards and bank account numbers, but health insurance policy numbers are also prime targets for thieves. An estimated 1.84 million people were victims of medical identity theft in 2013, according to the Poneman Institute, a research organization, which expects that number to rise.

Victims often don't realize they've been targeted until they discover a drop in their credit score or until a collection agency comes after them for unpaid medical bills, says Jim Quiggle, director of communications for the Coalition Against Insurance Fraud, a group that includes insurers, consumer activists and government officials. While most of the cost of medical identity theft is borne by the health-care industry and government, the Poneman Institute estimates that about 36 percent of victims in 2013 incurred out-of-pocket costs such as reimbursements for services provided to impostors, legal fees and identity protection services. The average cost for these victims amounted to \$18,660; in a few cases, it exceeded \$100,000.

Medical identity theft can happen in several ways. In one common scenario, the criminal persuades a consumer to divulge his health insurance number. Strategies for collecting these numbers can be highly sophisticated, especially when crooks operate in teams, Quiggle says. "They might invite seniors to bogus health fairs where they take their blood pressure and give them some nutritional supplements and ask to see their Medicare cards."

Jennifer Trussell, who investigates medical identity theft for the Department of Health and Human Services' Office of Inspector General, has seen cases where criminal rings target senior centers or homeless shelters and offer people \$50 for, say, their Medicare number. "That information is sold again and again," she says.

Even though the victims in these instances voluntarily share their numbers, they may not realize the impact, Quiggle says. "They'll discover to their horror that their Medicare account is being rifled and even maxed out by thieves who are making false claims against their policy."

Some cases are perpetrated by employees of medical offices or even health-care providers. Trussell worked on a case involving an Iowa chiropractor who had lifted the names and dates of birth of more than 200 patients to collect

"Victims often don't realize they've been targeted until they discover a drop in their credit score or until a collection agency comes after them for unpaid medical bill," says Jim Quiggle director of communication for the Coalition Against Insurance Fraud.



Coalition Against Insurance Fraud

fraudulent Medicaid payments. In another case, a Baltimore pharmacy owner and two employees were indicted for allegedly submitting bogus claims for prescription refills to Medicaid and Medicare.

Electronic medical records make your medical data easier to steal, because any clerk with access to patient records can load patient information onto a thumb drive and sell it to cronies or crime rings, Quiggle says. And because the Internet makes electronic records easy to share, tracking down all the providers who have received incorrect data can be difficult.

So how do you protect yourself? Never give your medical identity credentials to anyone but those with a legitimate reason for needing this information, such as the billing person at your doctor's office, Quiggle says. Treat with suspicion anyone who asks you for your insurance number without a good reason, and never give these numbers to telemarketers or callers conducting "health surveys."

Closely scrutinize the "Explanation of Benefits" or "Medicare Summary Notice" documents that are sent to you to make sure that you actually received the services and products listed, he says.