

## Medical Identity Theft on the Rise

A recent story in *Reader's Digest* November 2006 issue stated that in March 2004, Joe Ryan got a collection notice from a billing agency for Littleton Adventist Hospital near Denver, Colorado. The hospital wanted payment for surgery totaling \$41,188. Ryan, a Vail pilot, had never set foot in that hospital. Obviously there was some mistake. "I thought it was a joke," says Ryan.

But when he called the billing agency, nobody laughed. Someone named Joe Ryan, using Ryan's Social Security number, had been admitted for surgery. Ryan thought it would only take a few phone calls to clear up this matter. Two years later, Ryan continues to suffer from the damage to his credit rating and still doesn't know if his medical record has been cleared of erroneous information. "I'm desperately trying not to go bankrupt," he says.

Joe Ryan *is* the victim of a little-known but frightening type of consumer fraud that is on the rise: medical identity theft. Unlike financial identity theft, where crooks steal your personal information to rack up bogus credit card and other charges, medical identity theft involves using your name to get drugs, expensive medical treatment and even fraudulent insurance payouts.

For some unfortunate victims, medical identity theft is the last straw; after crooks steal their wallet and max out the credit cards, they turn to the health insurance card for even more freebies. "An insurance card is like a Visa card with a \$1 million spending limit," says Byron Hollis, national anti-fraud director of the Blue Cross and Blue Shield Association. Incidents often go undetected or unreported, but comprehensive research conducted by the World Privacy Forum suggests anywhere from 250,000 to 500,000 Americans have already been victims. It's hard to tally the cost, but fraud is estimated to account for as much as ten percent of all health care costs. How much of that is from medical identity theft is unknown.

As Ryan discovered, money isn't the half of it. When someone steals your name to receive health care, that person's medical history becomes part of your record. Setting the record straight can be extremely difficult because, in part, the information is dispersed among dozens of caregivers, from doctors to pharmacies to insurance companies and labs.

Incorrect entries can prevent beneficiaries from getting insurance, disqualify them for some jobs, and even lead to injury or death. Imagine arriving at the ER with a ruptured appendix, and your medical record shows (erroneously) that your appendix has already been removed. Doctors might waste valuable time looking for other causes.

To make matters worse, medical identity theft is largely a hidden crime. Some people find out through billing agencies, or when insurance companies send "explanation of benefits" letters that include obviously fraudulent claims. Still others learn when insurance coverage is denied because they have inexplicably reached their benefit cap, or when their records indicate a life-threatening disease they don't have. Many more people may never realize they've been targeted by more sophisticated crooks, who change billing addresses and phone numbers to avoid detection.

TRICARE beneficiaries are not immune to ID theft! Case in point: Medical ID theft was reported by HMHS regarding an imposter receiving medical benefits by using a stolen military dependent identification card. The real beneficiary, Jacob M, age 20, denied receiving the services. HMHS discovered the imposter would be receiving outpatient care and coordinated with this office and DCIS to initiate a "sting operation." After failing to show up for a scheduled appointment, Donald R, the imposter, was arrested two weeks later while seeking treatment at Green Oaks Medical Hospital on a "John Doe" warrant. injury or death. Imagine arriving at the emergency room with a ruptured appendix, and your medical record shows (erroneously) that your appendix has already been removed. Doctors might waste valuable time looking for other causes.

This office recently received a copy of the Plea Agreement. Donald R pled guilty on March 23, 2006, to one count of False Claims to the Government. On August 23rd Mr. R was sentenced to two years probation, refrain from incurring new credit card charges, participate in a program for treatment of narcotic, drug, or alcohol dependency, including testing, participate in mental health treatment services, and pay restitution in the amount of \$8,762.87.

It is recommended beneficiaries follow the following safeguards to protect their medical IDs:

- 1. Treat your ID card like a credit card.** Don't lose it or loan it, and don't show it to anyone except a trusted health care provider.
- 2. Watch out for "freebies."** Be suspicious of offers for free medical care. Avoid clinics that advertise aggressively,

promise to waive co-payments, provide free transportation, or similarly entice you.

**3. Ask for and Read the EOB.** Carefully review it and call about claims for services or drugs that you don't understand.

**4. Check your benefits yearly.** Once a year, request a listing of benefits paid out by your insurer. That way, you'll discover fraudulent payments even if the thief has changed your billing address.

**5. Request an accounting of disclosures.** You have a right under HIPAA to get this document from every health care provider you visit. The accounting will detail what personal information was released and whom it was sent to. It's a good way to catch and track theft, because any fraudulent medical information will probably be passed along to other providers.

**6. Review your credit report.** If someone has stolen your medical identity and racked up unpaid hospital bills in your name, the charges could turn up on your credit report.