








Your Medical Records, Stolen!

How to protect yourself.

By Max Alexander
From [Reader's Digest](#)

November 2006

 EMAIL  PRINT  SUBSCRIBE to RD FONT    

ID Thieves' New Target

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 indeed been admitted for surgery. A busy man, Ryan was trying to get his new sightseeing business, Rocky Mountain Biplane Adventures, off the ground. He figured clearing this up would take just a few phone calls.

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 was 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.

Medical Identity Theft: On the Rise

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. It's not known how much of that is from medical identity theft.

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

Incorrect entries can prevent you from getting insurance, disqualify you for some jobs, and even lead to 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.

In 2000, Florida resident Linda Weaver told a Federal Trade Commission workshop that shortly after her daughter's wallet -- which contained a family insurance card -- was stolen, someone began receiving medical care in Linda's name. She was shocked to find her blood type had been changed in a hospital record. "It could have been tragic," she told the FTC.

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.

"It's clearly a growing problem," says Pennsylvania Attorney General Tom Corbett. "Medical care is very expensive, and there are people who just don't want to pay, or can't." So far, the cases in Pennsylvania have involved small-time drug peddlers and health care freeloaders. But already other states are seeing a disturbing connection with organized crime.

Experts point to several distinct versions of the crime that consumers should look out for.

When Bad Guys Get Sick

The Joe Ryan who checked into Littleton Adventist Hospital for surgery in May 2003 was actually Joe Henslik, a career bank robber, check forger and con artist with a long prison record. In 2000, Henslik was paroled from Colorado's Bent County Correctional Facility. He moved into the Centennial, Colorado, home of Jerry and Laurie Lips, whose son Justin had been a prison-mate of Henslik's.

Jerry owned Airport Journals, a publisher of aviation trade papers; soon Henslik was working there as an ad salesman. He obtained private information about Ryan, alleges Deputy District Attorney Brian Sugioka, when Ryan called to place an ad. Recalls the real Ryan: "He said send along a birth date and Social Security number with the check, and like an idiot, I did."

Two years later, the first hospital bill arrived. "I wanted to help straighten this out," says Ryan, "so I went to the hospital, and they had a three-inch-thick record for me, but they wouldn't let me see it. I showed them my ID, and they said that's not Joe Ryan's signature. Well, of course not! They had this other guy's signature."

Ryan had fallen into a victim's Catch-22: If your record doesn't appear to be yours, you may not have the right to see it, much less change it. The 1996 Health Insurance Portability and Accountability Act (HIPAA) gives patients broad privacy rights, as well as the right to examine their own medical records. But patients don't necessarily have the right to correct errors or even prevent errors from being passed along to other providers.

That's because health care providers aren't required to amend records that did not originate with them. Victims can spend years expunging bad entries only to discover a mistake that reappears later -- transferred from a record that wasn't noticed earlier.

Doctors are understandably reluctant to expunge any medical information from a file, because it could expose them to liability. For example, if a physician prescribed OxyContin for severe back pain, and the back pain wasn't in the patient's record, officials could question the reason for the prescription, which would still be on file at the pharmacy.

Ryan's next step was a visit to the Littleton Police Department, which conducted an initial investigation that included a recorded phone admission by Henslik. But the cops concluded there was not much they could do; local law enforcement has little experience with medical ID theft, and cases can end up being considered a civil matter.

Frustrated, Ryan went to the district attorney's office, but by then, Henslik was hospitalized under his own name with cancer (he died last December).

Desperation, Debt, and IDs

A spokesperson at Littleton Adventist Hospital says it worked closely with Ryan to ensure that he was not accountable for charges accrued by the man impersonating him. The hospital absorbed the loss and let Ryan off the hook. But Ryan says the whole affair made it impossible to grow his company: "Bankers would say my business plan sounds like a good deal. But then my credit became an issue."

A "Friend" in Need

Experts say a lot of medical identity theft occurs when desperate people needing health care steal insurance information from acquaintances or relatives. Marie Whalen, assistant vice president of ambulatory services at the University of Connecticut Health Center in Farmington, cites a case where a man with AIDS stole his cousin's ID and racked up almost \$80,000 in treatment over 15 years before confessing on his deathbed. The hospital had to reimburse the insurance company.

Recognizing the problem, UConn Health Center and other hospitals around the country now require photo IDs as well as insurance cards for non-emergency treatment. "You can't get on an airplane or cash a check without ID," says Whalen. "Why should health care be any different?"

UConn Health Center staff suspect that about a dozen impostors try to game the system every week: "We've had quite a few people say, 'I left my ID in the car,' and then they don't come back." Pennsylvania Attorney General Corbett predicts that insurance cards will eventually come with photos and signatures.

When Professionals Are Dishonest

But photo IDs won't stop one of the most insidious forms of medical identity thieves: insiders who fabricate care on real patients for profit. The crooks can be anyone with access to your medical info -- nurses, receptionists, pharmacists and, rarely, even doctors. The most egregious case involved Boston-area psychiatrist Richard Skodnek, who was convicted in 1996 on 136 charges and ordered to repay the government and insurance companies nearly \$1.3 million.

The case also reveals how difficult it can be to recover from medical identity theft. Among Skodnek's victims is the family of Debra Harritt of Natick, Massachusetts. In 1991, after suffering a family crisis, Harritt and her then-husband began seeing Skodnek. Shortly thereafter, the couple split up, and Skodnek was arrested for Medicare fraud. Soon Harritt discovered that Skodnek had been double-dipping -- billing Blue Cross Blue Shield for visits that she and her husband had paid for out of pocket.

But the worst was yet to come. Skodnek gave Harritt's son and daughter, whom he'd never seen, psychiatric diagnoses and billed Blue Cross.

Harritt, who testified against Skodnek, spent months trying to get her kids' medical and insurance records corrected. "Theoretically, that information was removed," says Harritt. "But a woman at Blue Cross admitted that the information was probably still archived in backup computer files."

Skodnek lost his license to practice medicine in Massachusetts, was barred from participation in federal and state health care programs, and served time at the Allenwood Federal Penitentiary -- "the one they call the Country Club," notes Harritt with a sigh. "I wanted him to do hard labor."

Ganging Up on Patients

Medical ID theft is beginning to attract organized-crime rings, adding a new dimension to the problem. Last year, California authorities busted a group led by Ukrainian twin brothers Alexander and Leonid Dzhuga, who had allegedly set up a phony health clinic in Milpitas, near San José.

According to the indictment, the Dzhugas and their associates lured Medicare patients to the clinic by dangling free transportation and baby formula. Phony doctors performed cursory exams and ordered ultrasound tests, then billed Medicare. Meanwhile, patients had no idea their medical information was copied so more fake treatments could be filed. (The defendants are awaiting trial.) Experts say organized medical fraud can be particularly damaging because the theft is deliberately spread among numerous patients, using small, routine claims like ultrasound exams to avoid detection.

So What's to Be Done?

Reining in medical identity theft won't be easy. The Department of Health and Human Services is developing four prototypes of a so-called National Health Information Network that would make electronic health records instantly available in real time to caregivers everywhere. The laudable goal is to speed the flow of lifesaving information. But fraud experts are concerned it could open the door to even more

identity theft. Earlier this year, the Government Accountability Office noted "significant weaknesses in information security controls" in Medicare and Medicaid claims processing, which has already been digitized.

Meanwhile, the World Privacy Forum is urging regulatory changes that could provide recourse to victims. Among their recommendations are free copies of medical records for victims, more flexible rules to allow the victims to amend their records, and better accounting when providers disclose medical information to other providers, a key way to track down mistakes. The forum is also calling for new ways to track medical care given in a patient's name after a data breach occurs.

For now, says Hollis of the Blue Cross and Blue Shield Association, "our No. 1 defense is the consumer himself. We send out explanation-of-benefits notices, and people round-file those right off the bat. If people would look at those, a lot of theft would get caught."

But not all. Debra Harritt, who paid close attention to her benefits, didn't realize what was going on until Skodnek was arrested. "People think this is about big insurance companies," says Harritt, "but there are real victims -- real people who went through pain."