

Diagnosis: Identity theft

The medical field isn't immune to this growing 21st-century crime. For \$60, a thief can buy your health records and use them to get costly care. Guess who gets the bill?

By [BusinessWeek](#)

When Lind Weaver opened her mailbox one day in early 2004, she was surprised to find a bill from a local hospital for the amputation of her right foot. Surprised because the 57-year-old owner of a horse farm in Palm Coast, Fla., had never had worse than an ingrown toenail.

After weeks of wrangling with the hospital's billing representatives, Weaver stormed into the medical center and kicked her heels up on the desk of the chief administrator. "Obviously, I have both of my feet," she told him.

Weaver eventually persuaded the hospital to drop the charges but in the process discovered that the mistake wasn't a simple billing error. Weaver's identity had been stolen by a thief who had used her personal information -- her address, Social Security number and even her insurance identification number -- to have the expensive procedure performed.

The nightmare didn't end there. When Weaver was hospitalized a year later for a hysterectomy, she realized the amputee's medical information was now mixed in with her own after a nurse reviewed her chart and said, "I see you have diabetes." (She doesn't.) With medical data expected to begin flowing more freely among health-care providers, Weaver now frets that if she is ever rushed to a hospital, she could receive improper care -- a transfusion with the wrong type of blood, for instance, or a medicine to which she's allergic.

"I now live in fear that if something ever happened to me, I could get the wrong kind of medical treatment," she says.

250,000 victims

Weaver's experience isn't an isolated case. Medical identity theft -- in which crooks impersonate unsuspecting individuals to get costly care they couldn't otherwise afford -- is growing.

Based on Federal Trade Commission surveys, Pam Dixon, the executive director of the World Privacy Forum, a San Diego research group, estimates that more than 250,000 Americans have had their medical information stolen and misused in recent years. And this isn't petty larceny. Experts note that though individuals who have had their credit card data stolen are usually wrangling with their banks over losses of as little as a few thousand dollars, medical ID theft can leave victims, and the doctors and hospitals that provided the care, staring at bills that are exponentially higher.

Yet the thief isn't always an individual desperately needing medical care. In some instances, the perpetrator can be a doctor hoping to pad his or her income by filing fraudulent claims. Even worse, law-enforcement authorities say that more frauds are being perpetrated by organized crime rings that steal dozens, and sometimes thousands, of medical records, as well as the billing codes for doctors.

The rings then set up fake medical clinics --- offering free health screenings as a ruse to draw in patients -- that submit bogus bills to insurers, collect payments for a few months and then disappear before the insurers realize they've been had. (Dixon notes that health records fetch \$50 to \$60 each on the black market versus a mere 7 cents for stolen résumés.)

'Yesterday's drug dealers'

Last year, California authorities busted a ring in Milpitas, Calif., that had recruited patients from a local senior-citizen center with offers of free checkups and cases of Ensure nutritional supplement. In the three months before authorities raided the clinic, the ring had billed \$900,000 for diagnostic tests it had never performed.

"Yesterday's drug dealers are now working in today's health-care fraud," says John Askins, an investigator in Florida's insurance-fraud division. "It's more lucrative, and they don't face the same dangers they do in the narcotics trade." The penalties, if they're caught, are lower, too.

Health-care providers say the Bush administration's initiative to push doctors and hospitals to convert their paper-based patient files into digital records should help reduce the number of medical ID frauds. "Our software has become more sophisticated, particularly in identifying spikes in usage -- someone who normally goes to the doctor once a year and suddenly goes 25 times in a 12-month period. It's a red flag," says Byron Hollis, the national anti-fraud director for the Blue Cross Blue Shield Association, a trade group for 39 health plans.

But some privacy advocates fear that the rush toward digital health records could ironically create new nightmares for victims of medical ID theft. Rather than residing in a single doctor's paper files, fraudulent information -- such as the erroneous diabetes diagnosis in Lind Weaver's records -- could

circulate in other medical databases across the country. Given that some medical ID thefts are "inside jobs," wherein rogue clerks sell patient data to crooks on the outside, privacy advocates believe that allowing data to flow more freely around a national network could make such thefts even easier. "We can expect (medical ID theft) to grow the more we move toward an electronic health-care system. It's going to be a disaster," says Dr. Deborah Peel, an Austin, Texas, psychiatrist and the founder of the Patient Privacy Rights Foundation.

Even worse, it can be difficult for patients to purge any fraud from their records. Though the Fair Credit Reporting Act gives victims of financial identity theft the right to see and try to correct any mistakes in their credit records, critics say that victims of medical ID theft don't have the same recourse. Health privacy laws "are limited and don't reflect the possibility of medical ID theft," notes Robert Gellman, a leading privacy consultant in Washington. "Negative information could just bounce around the system forever."

Lingering consequences

For some victims, the pain is real. Take the case of Joe Ryan. In early 2004, the 60-year-old owner of a Colorado sightseeing business -- he flies passengers in a replica of a 1939 biplane -- got a bill from a hospital outside Denver. The hospital was seeking \$41,188 for surgery that Ryan says he hadn't had performed. Ryan called the hospital and, in time, realized that someone had stolen his personal information to pay for the surgery. Eventually, investigators traced the crime to a former clerk at a newspaper in which Ryan had placed an ad for his sightseeing business. "He asked for my Social Security number, and I now realize I shouldn't have given it to him," Ryan says.

When Ryan tried to correct his records, he discovered how difficult it can be for victims to clear their names. The hospital wouldn't let him see his own medical records when they determined that the signature on the driver's license Ryan handed them didn't match the signature that the perpetrator had used when he checked in.

"They said I couldn't be Joe Ryan," he recalls. Though the hospital eventually absorbed the loss, Ryan says he hasn't been able to erase the supposedly unpaid debt from his credit record. With his credit ruined, Ryan says, he had to pay a stiff interest rate -- 6 points over the prime rate -- when he refinanced his plane, and his insurance company has jacked up his premium.

"It has been like a glacier moving over me," he says. "I'm just screwed because I'm going to lose my airplane, my business and my credit rating."

In other instances, the thief can be a patient's own doctor. Debra Herritt discovered that after she and her husband began seeing a Boston psychiatrist, Richard P. Skodnek, in the 1990s. After two years of therapy, Herritt began receiving statements from her insurer, Blue Cross & Blue Shield Association of Massachusetts, showing that Skodnek had billed Blue Cross for sessions the Herritts had already covered. What's more, Herritt learned that Skodnek had also billed her son and daughter for psychiatric sessions that Debra says never occurred. "My children had never laid eyes on him," she says. Fortunately for Herritt, federal investigators were already on Skodnek's trail for defrauding other patients, and in 1996 the psychiatrist was convicted on 136 counts. Even then, Herritt says she spent the next couple of years trying to convince Blue Cross that her children had never been treated for depression.

"It was an incredible invasion of their lives," Herritt says now. "I just pray this doesn't come back to haunt them somewhere down the road."

'You'd be astonished'

Law-enforcement authorities complain that many health-care facilities do too little to protect their patient data. Case in point: In September, federal authorities arrested a scheduling clerk at the Cleveland Clinic's Weston, Fla., hospital who allegedly had passed on the personal identification information of more than 1,100 patients to her cousin -- who in turn submitted \$2.8 million in false claims to Medicare.

"Hospitals have done a poor job of implementing security procedures on their computer systems," one federal investigator says. "You'd be astonished how many people have access to your medical records."

Cleveland Clinic officials say they notified law-enforcement officials when fraud was detected in June and that they've since conducted an internal risk assessment to prevent such a problem in the future.

In their defense, health-care executives say they've taken steps in recent years to deter identity thieves. Some hospitals, for instance, have begun reprogramming their computer systems to restrict staffers from accessing any patient data beyond what they need to do their jobs. Some have instituted procedures to ensure patients are who they claim to be.

Among them is the University of Connecticut Health Center in Farmington. After one patient impersonating a distant relative gained admittance and ran up more than \$76,000 in bills in his cousin's name, hospital administrators two years ago began requiring anyone seeking treatment to produce picture identification.

"We've since had instances where patients say, 'I left my ID in the car,' then leave and never return," says Marie Whalen, the center's assistant vice president for ambulatory services. Beginning in March, Whalen says, the center will begin scanning these picture IDs into their files to help staffers confirm each patient's identity on subsequent visits.

"Most people are fine with that," she says. Indeed, it may be a small price to pay to avoid ID theft.