

WSJ's Health Journal: Identity thieves find ways to target patients

Wednesday, February 23, 2005

By Kevin Helliker, The Wall Street Journal

A sudden tear in his aorta required Robert Parker to undergo emergency open-chest surgery. As he recovered in the intensive-care unit of a California hospital, a Nevada criminal began seeking credit using Mr. Parker's name and Social Security number. That information was at the front of his medical file, which was visible to hospital personnel.

Was that a coincidence?

Certainly, identity theft isn't among the risks of medical treatment -- such as infection -- listed on the standard release form that patients sign. But there's evidence that identity thieves are starting to target medical patients.

Just this weekend, the University of Chicago Hospitals reported that a former employee had stolen identity information from as many as 85 patients. In recent years, rings of thieves stole the identities of more than 15 such patients in Iowa, 30 in Minnesota and nearly 50 in Indiana. During the past two years, the state of Michigan has prosecuted more than 20 cases involving medical-patient identity theft, many involving multiple victims, Michigan Attorney General Mike Cox says.

Hospital patients are vulnerable in part because they are unlikely to detect anything amiss. Some may never leave the hospital. A team of alleged identity thieves arrested in 2003 in New Jersey were targeting the terminally ill, according to police.

The biggest vulnerability of hospital patients is that their Social Security numbers often double as a medical identifier. For identity thieves, "Social Security numbers are the key to the golden kingdom," says Mari Frank, a California attorney specializing in identity theft.

Of course, new technologies such as bar-coded wristbands and electronic medical records accessible only by password will help thwart identity theft. And the recently enacted Health Insurance Portability and Accountability Act, or HIPAA, pressures hospitals to improve patient privacy, and is expected to bring improvement. But social security numbers often continue to be used as patient identifiers.

Often, the culprit in medical settings is a rogue employee. Identity-theft experts recommend that patients and loved ones protest any visible use of Social Security numbers, such as on wristbands or unguarded charts. At the very least, patients may be able to darken a couple of numbers. Patients should refuse to answer aloud any verbal request for those numbers when they might be overheard.

Patients should also resist the impulse to trust their fellow patients. "If you and the other guy were at the counter at Costco, you'd be careful in a way that you're not when you're wearing hospital gowns," says Mr. Cox, the Michigan attorney general. His office recently extracted a guilty plea from a cancer patient who stole the identities of nine other cancer patients.

Victims of identity theft should also tell police about any recent stay in the hospital. That's about the only way police can begin to see a pattern in a crime that typically is random. Often, identity theft happens when criminals simply get their hands on a stolen wallet or some discarded credit-card receipts.

Ultimately, a person whose identity is stolen isn't held responsible for debts racked up by crooks. But clearing one's name and credit record can take months, even years, and cost thousands of dollars, not to mention taking an emotional toll. The impact of identity theft upon the ill remains unmeasured. But "clearly it's the last thing they need," says University of California/San Diego psychologist James Kulik, who has published research on the psychology of surgical recovery.

For Mr. Parker, the difficulties of his recovery were deepened by worry about the sudden pile of debt that a credit-card company, cellular-phone service and real-estate firm were carrying under his name. "I'd wake up in the middle of the night thinking, 'I'm going to get sued,'" he recalls.

Some victims conduct their own investigation -- as did leukemia patient Eric Drew after his identity was stolen. When Mr. Drew learned that a department store possessed a video showing the individual using Mr. Drew's identity, he persuaded the store to give him a copy of the tape. Then, Mr. Drew beseeched a local television station to run the footage. Several callers identified the criminal as a lab technician at Seattle Cancer Care Alliance, where Mr. Drew was being treated.

Seattle Cancer Care Alliance said it never determined how its employee obtained Mr. Drew's information but that "The SCCA is confident that the measures we have taken to further secure our patient information systems will help to protect our patients from any such event in the future."

In the case of Mr. Parker, the aerospace engineer suspects his identity was stolen by a temporary nurse staffing the intensive-care unit at Little Company of Mary Hospital in Torrance, Calif.

A hospital spokeswoman, Beverly Wishon, says the hospital found no evidence that Mr. Parker's identity was stolen within its corridors. However, she says that nurses had access to Mr. Parker's Social Security number, and that the hospital sometimes employs temporary nurses. She also says that Little Company of Mary is changing its system so that Social Security numbers won't be available to anyone outside the billing office.