Health Information Compliance Alert

Industry News: Medical ID Theft: Is Anyone Safe Anymore?

The good news is staying out of harm's way takes just a few precautions.

Electronic health records may carry a hidden risk for patients: heightened exposure to medical identity theft, according to a post on www.healthcareinfosecurity.com. "The shift to EHRs probably happened faster than the organizations' abilities to understand the security implications and react to them," says **Matt Marshall**, vice president of security at **Redspin Inc.**, a Carpinteria, Calif.-based consulting firm.

"If the industry doesn't take security seriously, there will be an erosion of trust in healthcare," warns **Mike Spinney**, senior privacy analyst with **Ponemon Institute**, a Traverse City, Mich.-based research firm.

The post talks about a recently conducted survey by Ponemon which showed that an alarming 9 percent of respondents had experienced Medical ID theft in some form: directly or through an immediate family member. (To read about the survey, visit: www.healthcareinfosecurity.com/articles.php?art_id=2271.)

We Say EHRs, Hackers Spell It C-A-S-H

According to Marshall, hackers view EHRs as "electronic stacks of cash because they represent high-value data to sell on the black market."

A hacker gets around 40 cents for a stolen credit card number, and a stolen medical identity fetches a premium price of $14 to $18, says Marshall in the post.

"If I steal a credit card number, I can create a fake card and use it a few times. If I can get your full identity, I can open up many accounts, max out your credit and use it for a number of malicious activities. And it's much harder to shut that down; it's not as simple as canceling a credit card," he says Medical ID theft is therefore a "much more sinister crime" than credit card fraud, according to Spinney. Once a hacker has access to the wealth of information, such as Social Security numbers, images of drivers' licenses and insurance cards, and full medical histories, stored in a healthcare organization's computers, they can do a lot of damage, he argues.

This information, for instance, can be sold to illegal aliens for obtaining employment. Or to the uninsured for obtaining healthcare coverage. And the scariest part is medical ID thefts can stay ndiscovered for a long time. In the Ponemon survey, 52 percent of the theft victims said they took a year or longer to discover the crime. And the average theft cost the victim $20,000. Scary numbers indeed.

So, Identity Theft Is Happening. What Now?

Both Spinney and Marshall say on the post that it's time hospitals and clinics started dealing with information security on a priority basis. For example, they say organizations should:

• Start educating staff members about the threat of medical ID theft;

• Create comprehensive risk management programs;

• Designate someone to enforce security policies; and

• Assess the security policies of business associates.

But at the end of the day, they say, it boils down to plain old fashioned common sense. Paying attention to small details, such as not leaving a laptop behind in the back seat of a car, can have a big impact.

(**Editor's note**: To read the complete post, visit: www.healthcareinfosecurity.com/articles.php?art_id=2314&pg=1.)