

New IT buzzwords: 'medical identity theft'

January 22, 2007 | Eric Wicklund, Managing Editor

ST. PETERSBURG, FL - "Interoperability" and "transparency" may be two of the more prevalent buzzwords in healthcare IT these days, but a simple three-word phrase could trump them in importance during the coming year: Medical identity theft.

It's defined as the obtaining by theft or deception of personal medical information, such as one's address, social security number or health insurance information, for use in submitting false claims or seeking medical care or goods.

Since the beginning of 1992, the Federal Trade Commission has logged 19,428 complaints involving medical identity theft, and those studying the problem feel the number of cases is much higher.

The incidents are piling up almost daily. In December, Deaconess Hospital in Evansville, Ky. reported the disappearance of a laptop from its respiratory therapy department that contained personal information in 128 patients. In North Carolina, seniors were alerted to a scam involving phone calls from a supposed insurance company telling them their Medicare prescription plan's premium hadn't been received due to a computer glitch and asking them for personal information. And a Nov. 23 burglary at the offices of Electronic Registry Systems, Inc. in Cincinnati resulted in the theft of personal data from five hospitals in Georgia, Pennsylvania and Ohio.

In a Spring 2006 World Privacy Forum report, executive director Pam Dixon concluded that anywhere between 300,000 and 3.25 million people have been affected by medical identity theft. Those numbers, in turn, prompted EpicTide, a St. Petersburg, Fla.-based vendor of IT security solutions, to commission a survey that measured people's comprehension of medical identity theft.

That survey, released Dec. 12, contained some disturbing news.

Conducted last November by The Benchmarking Company, an independent research firm, the survey polled 500,000 consumers on 23 questions relating to medical identity theft and received 507 responses. Among the most surprising results, said EpicTide CEO Kurt Long, was the number of respondents (2.7 percent) indicating they had been victims of medical identity theft.

"This is a phenomenon that appears to be happening more frequently," he said.

Part of the problem, Long says, is that people don't know what medical identity theft is or they don't care much about it. According to the survey, 47.7 percent had never even heard the term before, while only 52 percent agreed that "allowing a family member to use their insurance card to receive medical care," is an example of medical identity theft.

Long believes medical identity theft isn't being taken seriously enough even though "it's the first information crime that could actually jeopardize your life." Part of the problem, he says, is that most people affected by this crime don't even know who targeted them, making it difficult to seek any sort of retribution. He's suggesting a broad-based response that includes laws allowing victims of medical identity theft better access to their medical records, a coordinated effort by law enforcement to investigate and prosecute instances of theft, and more effort by healthcare IT companies and insurance firms to identify and prevent them.

Part of the problem in the healthcare IT industry, he adds, is that new advances are outpacing security procedures, and companies are leaving themselves open to theft issues in the name of transparency. That point was brought up by Dixon in her WPF report, when she questioned the viability of a National Health Information Network (NHIN).

“Currently, the mantra is that digitization of private records will improve healthcare, reduce fraud, reduce medical errors, and save lives,” she wrote. “But this does not account for the challenging reality of medical identity theft and the substantial problems it can introduce into such a system.”

“The point is, can we really, truly know how the system is being used?” asks Long.

He says the challenge in battling medical identity theft comes in understanding the crime, and points to data in the EpicTide survey that indicates the public doesn't really know what's going on. For example, of the respondents who were asked to sign a notice of their HIPAA rights at a doctor's office, hospital, pharmacy or medical organization, 88 percent said they understood their patient rights – and yet when asked true or false questions, 35 percent of the answers were incorrect. In addition, more than a third of the respondents think their medical records can be legally shared via verbal consent with family members, other doctors or members of medical organizations where they seek care. And almost 43 percent of those surveyed believe it is legal for employees of the medical organization where they seek care to look at their records without written consent or knowledge.

Finally, the survey points to a certain degree of skepticism or distrust. Only 40 percent of the respondents say they felt their healthcare providers could protect their medical records, while barely half of those who responded felt healthcare providers know when someone illegally accesses medical records. And only 30 percent feel hospitals are diligent about informing potential victims of suspected breaches and unauthorized access to patient records.

“This is going to be a learning process,” says Long.