



November 20, 2006

### **Fighting Fraud & Identity Theft in Radiology**

**By Elizabeth S. Roop**

*Radiology Today*

**Vol. 7 No. 23 P. 40**

*Identity theft in healthcare can take many forms, such as the Texas man who posed as a chiropractor and submitted more than 1,300 fraudulent claims for radiology services before being caught.*

Or in California, where Medicare beneficiaries were given fraudulent imaging exams and had false diagnoses inserted into their medical records. The scheme raked in nearly \$1 million.

In these cases, the perpetrators were captured and prosecuted. But the opportunities for criminals to steal medical identities are growing exponentially with the advancement of electronic medical records and Web-based information exchanges and applications, and the pressure is on for healthcare providers to take a more proactive role in protecting their patients' personal health information (PHI).

“At the core of everything, including radiology, is the simple idea that the more electronic records we have and the greater access we give to others because of competitive pressures to deliver efficient results faster, those two fundamental drivers will create a greater amount of risk and a greater number of security incidents that can harm patients and the institution,” says Kurt Long, founder and CEO of EpicTide, a compliance and information security company.

#### **Difficult Detection**

There are several types of identity theft in healthcare. Medical identity theft occurs when an individual steals another's identity to gain access to care. The perpetrator is typically an uninsured friend or relative in need of medical care, although a number of cases have been reported where the thief was a stranger who obtained the information from a healthcare worker or on the black market. Requesting a patient's valid photo ID before treatment can minimize your facility's exposure to this kind of theft. A related form of identity theft is someone fraudulently billing procedures or tests that are never done to someone else's insurance. This is different from someone using a stolen identity to steal service from a legitimate facility. In this scenario, someone in the facility is using their position to steal from payors.

PHI theft occurs when a person's identity is taken from information stolen from a healthcare entity. In this instance, the crime is usually perpetrated by a current or former employee who sells the information. Some cases involve data that has been compromised by hackers, computer thefts, etc.

The World Privacy Forum estimates that there are 250,000 medical identity theft victims, although that figure is most likely low. “It's very difficult to detect,” says Executive Director Pam Dixon. “A lot of people who have this happen to them find out [years] after the fact.”

Estimating the economic impact of medical identity theft is also complex. However, anecdotal evidence gathered by the World Privacy Forum suggests a range of \$1,000 to \$1 million per incident, with most complaints falling within the \$20,000 to \$150,000 range.

One man spent \$10,000 to clear his name after someone stole his identity and listed him as the father of her baby. “I told him he was lucky to get it cleared up,” says Dixon, citing other cases where efforts to clean up the mess have dragged on for years and left the victims bankrupt.

While financial identity theft victims spend an average of 30 hours cleaning up and recovering from the misuse of their personal information, evidence suggests it takes medical identity theft victims as long as 175 hours—if they succeed at all.

Even more frightening than the financial devastation are the long-term and potentially life-threatening implications of medical identity theft. In addition to being denied jobs and insurance coverage, victims whose medical records have been altered can be denied lifesaving care or receive incorrect care based on erroneous medical histories.

### **Providers Hurt Too**

And it’s not just the victims who are hurt by the crime. The healthcare provider also pays a heavy price, both from lost reimbursements for services rendered and from damage to the organization’s reputation, especially in the case of large-scale loss of data.

Medical identity theft is a fast-growing crime in this country, largely because PHI is a valuable commodity. Some estimate that the black market value of a name attached to medical and insurance information is as high as \$60, compared with just 7 cents for a resume.

And while perpetrators come from all areas inside the healthcare system—doctors, nurses, lab technicians, billing clerks, and private individuals have all been prosecuted—it is the interest of organized crime that causes Long the most concern.

“It can be as small as a couple of people who are trying to make a little money all the way up to a very sophisticated organization,” he says.

Organized crime rings have set up fake clinics or taken over existing operations. Real doctors who have been compromised or “fake” providers will be put in place to legitimize the operation, then potential victims are lured in with the promise of free exams to obtain identifying information, such as what occurred in California.

These clinics operate for a few months, then shut down and move on. Most prevalent in Florida, California, and New York, clinic takeover schemes thrive by focusing on filing small claims that are spread out across multiple patients to avoid suspicion.

“They’ll submit as many claims as they possibly can as fast as they possibly can and collect the cash as many times as they can, often through Medicare and Medicaid, and then shut the thing down,” says Long, adding that “healthcare has a big bull’s-eye on it right now.”

### **Freestanding Targets**

Freestanding diagnostic imaging centers in particular are at risk for compromise, both as take-over targets for organized crime and from internal theft, according to Long. Because they are independent and typically have a high patient volume and a small staff, there are fewer obstacles between criminals and victims.

“The collusion becomes easier,” he says. “There are not as many people involved; there are not as many checks and balances and there is not as much segregation of roles. Whenever you have that much power wrapped up in a few people’s hands, it lends itself to abuse.”

When it comes to investigating and prosecuting identity theft cases, who is responsible can be as hard to define as the crime itself. According to a presentation by Gail Sausser, Esq, staff attorney with Virginia Mason Medical Center in Seattle, at the 2006 National HIPAA Summit, the “enforcers” include the following:

- the Federal Trade Commission, which maintains a repository of identity theft complaints, provides victims assistance and consumer education, and brings enforcement actions against companies that fail to take appropriate precautions against security lapses;
- the Department of Justice, which prosecutes crimes involving intentional disclosure for fraudulent activity;
- local police, who investigate the crimes;
- state attorney generals, who protect consumers and enforce state laws;
- the Federal Bureau of Investigation, which investigates interstate crimes;
- the Secret Service, which was assigned responsibility for credit card crimes in the wake of 9/11 (they have a limit of \$2,000 before investigating a crime);
- the U.S. Postal Service, which investigates identity theft when mail is involved; and
- Health and Human Services’ (HHS) Office of Inspector General (OIG), which gets involved when cases of fraud involve federal healthcare programs and also maintains a hotline for reporting of fraudulent activities related to Medicare and other HHS agencies or programs.

### **Prosecutable When Caught**

But hotlines are just one way medical identity theft captures the attention of authorities. The OIG, which declined an interview request citing policies against discussing investigation processes, develops its own cases by working through Medicare carriers and other contractors. They are also brought in by other law enforcement agencies, when appropriate, and are sometimes notified of possible fraud by beneficiaries themselves.

The good news, according to Dixon, is that medical identity theft cases are “very prosecutable, once you figure out the medical record has been falsified.”

The bad news is that “one of the trends in law enforcement is to do everything electronically. Unfortunately, that’s not helpful in terms of identifying this particular crime. You’ve got to talk to the patients and ask, ‘Did you have these treatments?’ You really have to look at what on the medical record has been falsified and to do that, you have to talk to the person the record belongs to. That’s very expensive law enforcement and right now, no one is really doing that,” she says. “Even spot checking would pull up more cases. Right now, the easiest cases float to the top and [in] all the prosecutions I’m familiar with, they’ve won because [the crimes] were so egregious.”

### **Proactive Protection**

The black market value of an individual’s identity and the ease with which the crime of PHI theft can be concealed are not the only reasons medical identity theft is one of the nation’s fastest growing crimes.

According to Long, there are two reasons healthcare is a prime target for identity theft, the first being HIPAA—or more accurately, HIPAA’s perceived lack of teeth.

“HIPAA has been an amazingly positive legislation that has driven providers to improve security, and they have done that,” says Long. “But unlike other regulations, there have been no highly visible prosecutions or criminal charges brought against those who have violated HIPAA rules. What that tells outsiders is that while there are severe laws around identity theft in the financial arena ... there are no obvious repercussions for identity theft in the healthcare setting.”

The second reason is the highly collaborative nature of today’s healthcare environment, particularly the push toward creating electronic links between all providers. With imaging centers, hospitals, physicians, pharmacies, etc, all collaborating electronically, healthcare has become a very open-ended environment, which ultimately increases security risks.

That is why Dixon, Long, and other security and privacy experts are urging the healthcare industry to do a better job policing itself, starting with taking proactive steps to detect and prevent identity theft.

In a joint presentation to the Health Care Compliance Association's 2006 Compliance Institute, Donna Gilley, CCS, CCP, CHC, director of revenue cycle and regulatory compliance for LBMC Healthcare Group, LLC, and Wynelle Paige, RHIA, CCP, president of the Compliance Advisory Coalition, offered the following advice:

- request photo identification to validate identity before rendering care;
- store confidential information appropriately and limit access;
- keep computer monitors turned so the view of the screen is limited or use screen covers when displaying confidential information;
- keep passwords and log-ons secure;
- use shredders or locked shredding receptacles rather than trash cans to discard patient information;
- fax correctly, ensuring the number is correct and the fax is received by the authorized person;
- use encrypted e-mail for sending patient information outside the system;
- avoid discussing patient information in open areas where others can hear;
- conduct criminal background checks on all employees;
- maintain physical plant security; and
- make sure receipts for credit card payments are secure and do not keep credit card information in the patient's file.

### **Electric Fence**

On the electronic side, successful detection and prevention requires employee education, awareness, auditing, and daily monitoring of information systems to develop sustainable and affordable best practices.

Auditing and monitoring tools allow privacy officers and others responsible for protecting patient data to see when an employee, provider partner, or even a vendor is violating access policies or HIPAA regulations, then use that information as an education tool.

### **Management Buy-in**

Buy-in from both the executive team and the privacy team is critical and utilizing the information gleaned from ongoing audits to educate—not punish—employees will help create a corporate culture that is focused on patient protection, says Long.

“While we think this auditing and monitoring tool is amazingly powerful, it's only one part of [preventing identity theft]. You've got to get buy-in from management ... and you have to make concerted, multipronged effort from here on to protect the information lives of your patients and your institution or we're just going to see more and more of this,” he says. “It requires both a corporate culture and the ability to monitor because no matter what laws we have, without the ability to police, there are always people who cheat.

“A lot of this can come across as Machiavellian, but here's the truth ... as an executive, you want to trust people, but we can't let one or two persons with bad intentions jeopardize the overall institution for all of us, the employees and the stakeholders,” Long adds. “I look at it in this light; I may have to do a little more policing than I'd like, but I'm protecting the livelihood of my employees, of our donors, and our patients by doing that. We'd like to trust everyone down to the last man or woman, but we can't.”

— *Elizabeth S. Roop is a Tampa, Fla.-based freelance writer specializing in healthcare and health information technology.*