



Addressing the Growing Threat of Medical Identity Theft

HealthLeaders Magazine, By Kurt Long, for *HealthLeaders News*, October 12, 2006

A September *Los Angeles Times* report detailed the account of a Florida woman who refused to pay hospital bills she received for the amputation of her right foot. Since her right foot was intact, she was certain she had never received those services.

The erroneous diagnosis of diabetes was also added to the woman's medical records. An investigation determined that her medical information had been stolen, and someone else had received treatment under her name.

Healthcare leaders recognize that protecting patient health information is a vital component of patient safety, yet stories like that of the Florida woman persist. A 2003 federal report estimates that at least 200,000 incidents involving medical identity fraud occurred that year. Providers and payors face many of the same information security risks as financial institutions, including identity theft, which a Boston University study suggests may result in \$53 billion in annual losses nationwide.

Aside from the financial impact, risks to patients' well-being are escalating. A recent report issued by the World Privacy Forum finds that medical identity theft is a rapidly growing phenomenon in which the health and life of its victims are at stake. By understanding the nature of the crime and its various forms and by taking steps to educate employees about the importance of keeping patient information secure, hospitals can offer patients a more secure environment for their medical history.

Criminal activity

Medical identity theft occurs when a criminal obtains pieces of information about a person's identity, such as their name, address, social security number and health insurance information, then uses this information without the victim's knowledge to make false claims or fraudulently receive medical goods or treatments. Frequently, victims' medical information like blood type, prescription history, allergies or chronic diseases are changed as part of the false care being rendered. When a physician makes treatment decisions based on this erroneous information, the victim's life is endangered.

The increase in medical identity theft is being driven by the rising costs of healthcare coverage and services. Although identity theft may be perpetrated by individuals desperate for health insurance, more sophisticated and devious activities--like organized crime--are often at work. In many cases, a healthcare insider such as an unscrupulous physician, nurse, administrative employee or specialist works in collusion with the criminal and provides them with medical identity information for one or more patients. This information can be used directly or through a variety of schemes, such as an illegal clinic that runs up false claims, receives payment and closes its doors before authorities catch on.

In addition to medical identity theft, healthcare providers face a wide range of privacy breaches of a slightly less serious nature. Nosy employees may feel compelled to snoop on the medical records of other employees, facility executives, relatives and neighbors.

In September, New York City's public hospital system suspended 39 employees at Woodhull Medical and Mental Health Center after it was found that they had reviewed a patient's records without a need to do so. The incident involved a 7-year-old girl who had been abused in a highly publicized case. Because these highly damaging incidents almost always involve healthcare employees or insiders, information security measures must focus on more than simply keeping the bad guys out.

Deterring behaviors

Regulations under the Health Insurance Portability and Accountability Act of 1996 call for audit log reviews for every system that accesses protected health information so hospitals may anticipate common security incidents and develop operating processes that mitigate the damages of privacy incidents. The task of detecting a security breach falls to the privacy officer and to information security personnel. In many cases, privacy officers act on a tip from an employee or a complaint from a patient to search for discrepancies. But the mere detection of wrongdoing should not be where the stream ends. The executive management team must be keenly aware of the importance of patient information security and the repercussions for being lax.

When an incident is detected, the privacy officer should work with leadership to reinforce the serious nature of patient privacy, federal and state laws on privacy, as well as the organization's internal policies to all employees--whether they were involved or not. If the incident is minor and relates more to curiosity than to crime, it should be used as a teaching opportunity for the employee in question. If the incident is more serious or involves a repeated offense, the consequences for the employee are raised.

Once you crack down on even minor discrepancies, you'll find that word quickly spreads within the organization that the privacy office is able to detect common privacy violations and healthcare information security risks. The net result is deterrence and an associated decrease in incidents.

Continued troubles for victims

Until healthcare providers are able to make identity theft a thing of the past, victims will continue to pay a high price and face steep legal hurdles.

Although HIPAA has resulted in dramatic improvements in healthcare provider security, it also works against the victims of medical identity theft and risks making the healthcare industry even more susceptible to criminal activity. Unlike the financial services industry, healthcare organizations in violation of HIPAA have not faced highly visible prosecutions. Industry experts believe this makes healthcare an attractive target for all forms of identity theft.

The World Privacy Forum report finds that organized criminals, like those involved in drug trafficking rings in California and Florida, are turning to medical identity theft because they believe the penalties will be less severe than those they might face for traditional crimes.

It won't happen overnight, but stricter prosecution may be on the horizon.

In September, Oregon's Providence Health System agreed to pay more than \$95,000 to the state Department of Justice to settle a nine-month investigation relating to patient privacy. Providence lost 365,000 patient records on computer disks and tapes and had previously agreed to pay \$7 million to \$9 million to victim credit protection services.

The victims of medical identity theft have little recourse to clear their medical records. The resultant medical and professional complications can last for years. The Florida woman who was billed for a non-existent amputation has spent more than a year trying to clear her medical records and has spent as much as 40 hours per week attempting to do so.

Kurt Long is CEO of EpicTide, a St. Petersburg, Fla.-based compliance and information security company. He may be contacted at kurt.long@epictide.com.