Damage of Medical Identity Theft

Save to myBoK

HIM Professionals “Single Most Important Group” in Finding Solutions

Medical identity theft can wreck the lives of its victims and cost healthcare organizations money and time. But HIM professionals can help mitigate this growing problem, according to Pam Dixon, executive director of the World Privacy Forum.

“Medical identity theft is a crime that harms patients and a crime that hides itself,” Dixon said. “I view you as the key individuals on the front lines of this crime and the single most important group to find and implement an appropriate response to the unique harms of medical identity theft,” she told attendees.

Speaking at Tuesday’s general session, Dixon told attendees what medical identity theft is, how it operates, and some of the best responses identified by the Forum.

What It Is, What It Isn’t

Medical identity theft occurs when someone uses the name or parts of the identity of another person—insurance information or Social Security number-without that individual’s knowledge or consent to obtain goods or services or to make false claims. From an HIM perspective, medical identity theft creates erroneous entries in a medical record, or a fictitious medical record, that can be very difficult to rectify.

Medical identity theft can be committed by an individual or a group of people, Dixon said. “It is not medical identity theft when someone steals a name from a medical record and goes shopping,” she noted, adding that while this act is an example of fraud, it is not the same thing as medical identity theft. Some examples of medical identity theft include:

- A woman who used her roommate’s identity to get prescription drugs for herself
- A group of fraudsters who took medical information from a clinic and used it to bill insurers for services never received
- A man whose wallet was stolen who found himself wrongly named as the father of a child he didn’t have and as a patient for services he did not receive
  When any of these occur, Dixon said, “You can have big problems.”

Few Remedies Exist

Changes to medical files can pose particularly serious problems for victims long after an identity theft occurs, she said. Victims may find themselves denied insurance coverage or fail pre-employment screenings as a result of medical identity theft, or they may find themselves saddled with debt for medical bills. It can take up to two years to detect a crime and it is “nearly impossible for victims to rectify, unless they get lucky,” she said.

Dixon added that while all patients are potential victims of medical identity theft, the elderly, chronically ill, or others who are in frequent contact with the healthcare system are most vulnerable.

Institutions, including providers and payers, are medical identity theft victims as well. “Providers also have to deal with the problems, but patients don’t have the same skills or tools to deal with medical identity theft that providers do,” Dixon said.

In May 2006, the Forum published a landmark report on medical identity theft. “The phones are still ringing today,” she said, with calls from people seeking help. From her research, Dixon says she has seen some patterns in the complaints from patients: they say they are unable to get a copy of their medical record and they say they cannot make amendments or corrections to inaccurate or fraudulent information.

“HIPAA does not help us here,” Dixon said. “It does not grant an absolute right of access to files or rights or deletion of information. It has loopholes and gaps that create insurmountable challenges for victims.”

In contrast, it’s relatively easy for people to cancel stolen or lost credit cards, because the financial industry is regulated by laws that protect consumers against these risks, Dixon said. There is no corresponding law that protects victims of medical identity theft or enables them to prevent fraud from happening again. Some healthcare organizations will not accept police reports from victims or are slow to launch medical identity theft investigations, she said.

In Search of Best Practices

Dixon said the Forum has worked with providers and experts to identify possible solutions, and a report detailing their recommendations is forthcoming. Among them:

1. Create a national set of processes to standardize how providers and insurers should handle medical identity theft. “We need uniform but appropriately flexible answers to important questions,” she said.

2. Create red flag alerts for medical records that prompt institutions to react in the potential presence of fraud.

3. Create “Jane/John Doe” file extractions in cases where fraud is substantiated. Information related to the fraud can be purged from a person’s medical record and held separately in a “Doe” file that is cross-referenced with the victim’s.

4. Have dedicated healthcare personnel trained to respond to medical identity theft incidents.

5. Remember that when medical identity theft is committed by insiders, asking patients to document their identity won’t help.

6. Consider medical identity theft issues in risk assessments, including “insider threat” scenarios.

7. Create materials to educate patients and providers.

As policy makers become more aware of medical identity theft, they are starting to create laws to address it. However, a patchwork of uncoordinated laws may not be the most effective way to reduce the problem, according to Dixon. “We get legislation when a community doesn’t handle its own problems,” she said. “This is the time to take action before others step in.”

Dixon said HIM professionals and AHIMA are well positioned to lead the effort. “You as HIM professionals can create a nationally accepted procedure for dealing with the aftermath of the crime from a victim’s perspective,” Dixon said. “I believe we can work together to greatly reduce these crimes.”

Article citation:
. "Damage of Medical Identity Theft" *Journal of AHIMA* 79, no.1 (January 2008): 58-59.