

Medical Identity Theft—Growing in Frequency with Devastating Consequences

by Leslie A. Fox, MA, RHIA, FAHIMA and Patty T Sheridan, MBA, RHIA

Thank you to Advance Magazine for permission to use this article

Leslie: The most commonly discussed identity theft cases involve credit cards and bank accounts, but today identity theft also includes obtaining medical care by using a stolen identity. The result can be devastating for a victim of this crime. The victim may be held responsible for paying the fraudulent bills and can be burdened with erroneous health information that is difficult to expunge from official records. Obtaining health and life insurance may become complicated or impossible because an electronic or paper health record may have been created reflecting a life threatening disease that the victim does not have. And more common, health care coverage is denied because the victim has reached his or her insurance benefit cap.

PATTY: It seems that medical identity theft is on the rise. Several of our HIM colleagues have had to address this issue within their organization. HIM professionals, working with IT, finance and legal etc. can help set policies and procedures to minimize and manage this issue within their organization. So we are on the same page Leslie, what is medical identity theft?

LESLIE: When we think about medical identity theft, we need to think of it as a subset of healthcare fraud. We also need to acknowledge that it includes two components: medical and financial.

Medical identity theft typically involves records of a thief becoming intermingled with records of an innocent victim. Thus, a victim's medical record could reflect a surgical procedure, medical diagnosis or health history that is that of the thief's. You can see how this might affect accurate treatment of the victim in the future and the insurance nightmares that could result.

Patty: Nightmare is an understatement! In preparing for our discussion today I searched the internet for some recent examples of medical identity theft. I couldn't believe what I found! Here are three examples that capture the flavor of this crime:

A 56-year-old retired Florida schoolteacher was billed for the amputation of her right foot. To deal with bill collectors and her insurance company, she sent notarized photos of her foot as evidence that her foot was still intact. If this wasn't enough, subsequently she was in the hospital about to receive a blood transfusion when the provider noticed the blood she was about to be given for a blood transfusion did not match the blood type in her medical record. The blood type had been changed previously to document the thief's blood type when hospitalized for their amputation surgery.

A Colorado man went to the hospital to address an erroneous bill he had received. When asked for his medical record, the victim was denied access. He was told that the signature on the record did not match the signature on his identification card. The victim pushed for an investigation, which he got, revealing an ex-con had stolen his identity. For over two years now, the victim has worked with healthcare providers to unmix his records with that of the ex-con.

A Pennsylvanian woman discovered she was a victim of medical identity theft when her insurance company denied a claim for a routine gynecological exam. The bill was \$189. It turns out that her identity was stolen by someone else who had a gynecology appointment under the victim's name. The appointment included an exam in preparation for an abortion.

LESLIE: I am familiar with some of these cases and it's alarming to me. I know there are many more examples that we can all learn from, not only as consumers of the healthcare system, but also as the guardians and managers of health information.

PATTY: Leslie, you mentioned earlier that one needs to also consider financial identity theft when thinking about medical identity theft. What do you mean by that?

LESLIE: The financial aspect of medical identity theft was included in some of the examples noted earlier and includes dealing with the hassles of unpaid bills and its affect on one's credit as well as ongoing letters and phone calls from health care providers and collection agencies.

PATTY: I can appreciate that this could be financially devastating at worst and terribly annoying at best.

LESLIE: Do you think the HIPAA law provides some protection or assistance under these circumstances?

PATTY: While HIPAA provides broad privacy rights including the right to examine one's own medical records, the reality is a provider is not likely to allow a victim access to their records. Imagine this scenario, someone asks to review their medical records because they don't think the information in the record is theirs. This results in the provider not allowing access since the information in the record does not belong to the person asking to see the records. Confusing!

Also if the victim's health information/medical record is part of a collection dispute, a provider is likely not to allow access to the medical record. In circumstances where access is given, it's likely that amendments are not allowed. Additionally, health information is transferred from provider to provider thus extending the reach of erroneous data. This makes amendments that much harder because providers are not obligated to amend records that did not originate with their organization and they are often reluctant to do so. It's very messy.

LESLIE: So where do we go from here as consumers and HIM professionals?

PATTY: Let's talk first about what HIM professionals can do to assist their organizations as well as victims.

The first thing I would suggest is for HIM professionals to raise the issue with key organizational leaders about developing medical identity theft procedures. More and more organizations want to help victims and also want to make sure that criminals don't game the system. HIM professionals can lead the way in developing practices that proactively deal with medical identity theft. Pam Dixon, the executive director of the World Privacy Forum suggests that organizations answer the following questions when designing their policies and procedures:

1. What do we do when a patient claims fraud in their file?
2. What do we do when a patient says the bills are for services the patient did not receive?
3. What do we do for patients and other victims when we uncover a fraudulent operation?
4. When we have a real case of medical identity theft, how can we work with patients to fix the records and limit future damages?
5. What can we do to prevent medical identity theft?

6. Who will be designated to work with victims and other parties such as the police?
7. What role can we play to educate patients about healthcare fraud in general and medical identity theft specifically?

LESLIE: I think the process of organizations formalizing their medical identity practices makes a lot of sense, especially because of the lack of laws and industry guidance in this area. It's in an organization's best interest to have a process for dealing with this issue and protecting their assets as well. What should organizations do to be more proactive? For example should they implement rigorous patient identity proofing processes?

PATTY: There is a lot of emphasis on patient identity proofing and while this is important, it may not be effective when it comes to medical identity theft.

LESLIE: That's interesting. Why do you think that?

PATTY: Medical identity theft is most often an inside crime. For example, there is a well known case where a front desk clinic coordinator downloaded 1,100 patient's names and their associated date of birth, social security numbers, Medicare numbers and home addresses and sold it to her cousin. This resulted in approximately \$2.8 million dollars in false claims to Medicare—not to mention the havoc it wreaked for victims who had to deal with false claims. Patient identity proofing would not have been effective in this instance.

LESLIE: This is a good example of the financial aspect of Medical Identity Theft. It sounds like in that case a good audit trail would have identified that data was being downloaded and should have raised suspicion.

PATTY: I do think it's important for organizations to address security weaknesses that may result in data breaches. Ensuring that access to data is monitored and that hardware is secure from intruders is a critical step in preventing medical identity theft. In addition, laptop security should be on everyone's radar because of widespread coverage in the news media. There have been a number of reported laptop breaches during the past several years. Laptops should include encryption of the hard drive and there should be policies around the removal of laptops that contain financial and health information management.

LESLIE: What about training the healthcare workforce and generally raising awareness?

PATTY: I think that is a good idea. It should be part of an organization's overall healthcare fraud training program.

LESLIE: There is so much more to discuss on this topic. I want to direct our readers to resources located on the World Privacy Forum (WPF) website at <http://www.worldprivacyforum.org/medicalidentitytheft.html>. The WBF privacy report is a good document for an organization to review and discuss as they set out to address this issue locally. It's also a good place to direct consumers as the report includes six things consumers should do to mitigate medical identity theft. These are: monitor the explanation of benefits, request an accounting of disclosures, request a listing of benefits from your insurer, request medical records, correct erroneous information and monitor one's credit report.

PATTY: A search of the internet on this topic produces many real world experience that hit close to home. As consumers there is a lot for us to consider about the importance of being vigilant about monitoring the information that will alert us to a case of medical identity theft. As HIM professionals, there is a role we need to play to help our organizations and consumers to thwart the bad guys.

LESLIE: I think we will be seeing much more about this issue and we can expect to see legislation introduced

at least within states in the future. The WPF site indicates that for the first time The Federal Trade Commission's (FTC) report on identity theft contains medical identity theft statistics. The FTC report indicates that three percent of the 8.3 million identity theft victims in 2005 were victims of medical identity theft. That means approximately 250,000 people were victims of medical identity theft in just 2005 alone! Clearly this is an important consumer and HIM practice issue for all of us to keep on our radar.

Leslie Ann Fox is chief executive officer and Patty Thierry Sheridan is president of Care Communications Inc., a national HIM consulting and staffing company headquartered in Chicago. They invite readers to send their thoughts and opinions on this column to lfox@care-communications.com or pthierry@care-communications.com.