Combating the Privacy Crime That Can KILL

Save to myBoK

By Joanne McNabb, CIPP/US, CIPP/G, CIPP/IT, and Harry B. Rhodes, MBA, RHIA, CHPS, CDIP, CPHIMS, FAHIMA

A Massachusetts man who was turned down for a job discovered that there was a false diagnosis of severe depression in his medical record. He ultimately learned that the information had been entered by a psychiatrist who was submitting fraudulent bills to insurers.

Elsewhere, a Seattle woman received a bill for the often abused drug of OxyContin, prescribed for her newborn son for a work-related back injury. She learned that her son's Social Security number had been stolen and used to obtain healthcare.

These are just two examples of medical identity theft—the fraudulent use of an individual's identifying information in a healthcare setting—which has been correctly identified by healthcare professionals as the privacy crime that can kill you. Not only does it inflict financial harm on patients, providers, and insurers, but it also corrupts records with erroneous information that can lead to incorrect diagnosis and treatment.

Medical identify theft's impact on medical records, and therefore on patients, is the focus of a new publication released by California Attorney General Kamala D. Harris. The guide, *Medical Identity Theft: Recommendations for the Age of Electronic Medical Records*, is one of the privacy best practices guides produced by the California Attorney General's Privacy Enforcement and Protection Unit. The Privacy Unit's mission is to protect the inalienable right to privacy conferred by the California Constitution by enforcing state and federal privacy laws, educating consumers, and encouraging businesses and other organizations to adopt best practices in the management of personal information. While the guide was developed by California state officials, it can also serve as a best practices manual for HIM professionals in other states to help stop medical identity theft before it harms patients.

"The move to electronic medical records provides an opportunity to address this serious quality-of-care issue," Harris says. "There are lessons to be learned from other industries that have experience in detecting and responding to fraud in electronic transactions."

In developing the *Medical Identity Theft* guide, the Attorney General's Office consulted with experts in the fields of health informatics, information security, patient privacy, medical records administration, and healthcare providers—including experts from AHIMA. Given the guide's focus on medical records, the expertise provided by AHIMA was of great value in developing the recommendations, California Attorney General Office employees found.

How Medical Identity Theft Happens

There are two primary ways in which medical identity theft happens. One is consensual: An individual may knowingly share his or her identifying information with a friend or family member in order to allow that person to obtain medical goods or services. According to a 2013 study by the Ponemon Institute, 30 percent of medical identity theft victims reported having shared their information with someone they knew.[1] This type is expected to decline as the Affordable Care Act extends healthcare coverage to many who are now uninsured or underinsured.

The other type of medical identity theft is perpetrated by someone unknown to the victim, including insiders in the healthcare industry. The impact on the victim's medical records is dangerous and potentially life-threatening regardless of the motivation behind the use of the identifying information and regardless of whether the fraud was perpetrated by a relative or a stranger.

Medical Identity Theft Difficult to Detect, Resolve

The crime of medical identity theft is often underreported, since it is difficult to detect, and can be misreported simply as healthcare fraud without healthcare professionals recognizing its impact on patient records. Nevertheless, it is clearly a significant problem, with the most recent study from the Ponemon Institute finding approximately 1.84 million victims in 2013, a 21 percent increase over the previous year.[2]

While knowledge of this crime has grown since it was first officially identified in 2006, not all healthcare organizations have adequate means for preventing, detecting, and remedying it in place. In addition, potential and actual victims of medical identity theft lack the rights and resources available to victims of financial identity theft to properly deal with the problem.

Consumers can detect financial identity theft by reviewing their credit reports, which they can do annually for free. As knowledge of financial identity theft has grown, consumer credit reports have become easier to read and understand. If a patient receives a bill that is the result of identity theft, he or she can dispute it with the creditor or collector, file a police report of identity theft, provide the police report to the creditor or collector and the credit reporting agencies, and have the item removed from the victim's credit report.

Dealing with the impact of identity theft on a victim's medical records is another story. Rights and resources analogous to those available to address financial identity theft include consumer-friendly Explanation of Benefits statements, free annual access to medical records, flags on compromised identities, easy access to records suspected of containing fraudulent information, and prompt correction of such information. But not all patients have equal access to this type of help and information.

First Aid for Medical Identity Theft

The California Attorney General's Office supplemented the healthcare industry-focused medical identity theft guidelines with an additional information sheet for consumers, "First Aid for Medical Identity Theft: Tips for Consumers." It describes five signs of possible medical identity theft and provides tips on what to do in response to each. Also included in the material are sample letters affected patients can send to providers and insurers. The consumer information sheet is available in English and Spanish on the Attorney General's website at www.oag.ca.gov/privacy/medical-privacy.

Signs of Possible Medical Identity Theft

- Receipt of a privacy breach notice from a healthcare organization
- Unknown item in an Explanation of Benefits statement
- Notice of reaching a health insurance benefit limit that you believe is erroneous
- Call or letter from a debt collector about an unfamiliar medical bill
- Questions about your identity or health conditions during intake at a doctor's office or hospital

Video Extra
Helping Consumers Combat Medical ID Theft

journal.ahima.org
The California Department of Justice released a list of five signs that your medical information has been breached. This video walks through immediate actions consumers and their HIM counterparts should take in the event of medical identity theft.

Industry-wide Mitigation Approach Needed

While patients can help prevent and mitigate medical identity theft when given the appropriate tools, the primary responsibility for addressing medical identity theft lies with the healthcare industry. The California Attorney General's guide offers specific recommendations for healthcare providers, payers, health information organizations, and policy makers.

The primary recommendation for providers is to build awareness of medical identity theft within their organizations and to implement an identity theft response plan. HIM professionals should show leadership by increasing awareness of medical identity theft threats organization-wide. They should offer to train admitting and registration staff on how to monitor for suspicious patterns or practices, such as a patient using suspicious driver's license or insurance cards, or a patient that knows their insurance number but doesn't produce an insurance card. Training should focus on real victim impact. Coding and business office staff should be trained to report medical record inconsistencies with regard to patient history or treatment and unusual billing patterns. HIM professionals should also provide consumer education on how to guard against theft—such as the importance of protecting insurance card information and the importance of monitoring statements from one's insurance company and healthcare providers. Public-facing posters could also be created that notes it is a crime to let another person use one's health plan card.

The mitigation plan should include a strategic use of technology as well as policies and procedures, with clearly defined responsibilities for staff. The guide provides recommendations for components of such a plan. The recommendations for payers also start with having a medical identity theft response plan in place, and include recognizing and taking action on the possible impact of fraud on medical records that first presents as financial-based identity theft. The health information exchange organizations being created to manage and oversee the exchange of health information have the potential to play a role in addressing medical identity theft. This can be possible if they adopt appropriate policies and encourage the development of standards, such as "red flags," to indicate suspect or compromised information in records.

Tackling the privacy crime that can kill requires collaboration among all healthcare industry stakeholders. The issues posed by medical identity theft should be taken into consideration as standards are developed for the healthcare infrastructure of the 21st century. Government policy makers and industry standard setters should consider electronic flagging capabilities and making a medical identity theft incident response plan a requirement for system certification.

Guide's Key Medical Identity Theft Recommendations

Regardless of healthcare setting or stakeholder obligation, organizations should develop and implement policies and procedures for the prevention, detection, and mitigation of medical identity theft. Staff understanding and adherence to organizational privacy and security policy and procedure is paramount to preventing medical identity theft. Implementation and enforcement of privacy and security measures ensures compliance and acts as a deterrent to theft.

Conducting regular compliance reviews and audits helps to detect and prevent inappropriate record access and security breaches. Notifying affected individuals of breaches accordingly and quickly promotes an organizational culture that embraces prompt mitigation of security incidents.

Recommendations for Healthcare Providers

- Build awareness of medical identity theft as a quality-of-care issue within your organization.
- Make patients aware of medical identity theft, which includes using someone else's medical ID or sharing theirs, and the potential consequences.
- Implement an identity theft response program with clear written policies and procedures for investigating a flagged record. Train staff in all relevant departments on these policies and procedures.
- Deploy technical fraud prevention measures such as anomaly detection and data flagging, supported by appropriate policies and processes so that all flags are appropriately investigated.
- Offer patients who believe they may be victims of identity theft a free copy of the relevant portions of their records to review for signs of fraud.
- When an investigation reveals that a record has been corrupted by medical identity theft, promptly correct the record. Use a procedure appropriate for the circumstances, such as removing the thief's information from the victim's record and placing it in a separate "medical identity theft file," or leaving the thief's information in the victim's record but flagging it as not belonging to the victim.

Recommendations for Payers

- Make Explanation of Benefits statements patient-friendly. Include information on how to report any errors.
- Notify patients who have been identified as victims of medical identity theft by e-mail, text, or another agreed upon timely method whenever a claim is submitted to their account.

- Use automated fraud detection software to flag suspicious claims that could be the result of identity theft.
- When medical identity theft is confirmed, the first priority should be correcting the patient's claims record to eliminate the possibility that benefits could be capped or terminated.

Recommendations for Health Information Exchange Organizations

- Build system capabilities that can assist in the prevention, detection, investigation, and mitigation of medical identity theft.
- Adopt policies and standards that recognize the possibility of medical identity theft. Include specific policies relating to medical identity theft as part of privacy and security policies and procedures.

Recommendations for Policy Makers

- When collaborating on the development of standards and software for electronic health records and health information exchange, consider the policies and procedures recommended in the California Attorney General's guide. The recommendations could also form the foundation of standard policies for industry self-regulation.
- The US Department of Health and Human Services should include a medical identity theft incident response plan as a certification requirement or as one of the best practices they are currently developing for health information exchange organizations and accountable care organizations.

Engaging Consumers in Preventing Medical ID Theft

Consumers face the greatest risks during a medical identity theft incident. Harm that can potentially come to patients impacted by medical identity theft includes a loss of privacy and confidentiality, denial of benefits, possible legal action or false arrest, loss of credit rating, lost time and money, and impaired health resulting from improper treatment.

Active medical identity theft is not always immediately apparent to a victim or a healthcare organization. A 2012 Ponemon Institute Survey revealed that 34 percent of victims reported discovering the crime one year after the incident. An additional 17 percent of victims reported discovering it two or more years afterwards.[3] Very often healthcare consumers are the first to become aware of fraudulent activities involving their health records or medical billing. When a patient presents with a complaint or question about a bill or about information in a medical record, the healthcare entity must be ready to consider that medical identity theft may be involved and follow up on it according to the facility's medical identity theft response plan.

The investigating organization must be ready with a workable process for capturing the information necessary to investigate the complaint from the patient. The process must ensure that the patient complaint is quickly sent to the appropriate department or individual. Once the necessary documentation has been gathered, the medical identity theft team should investigate by reviewing the patient's medical records, and other documentation including billing records, business associate stored records, and record-access audit logs. Investigators may also compare signatures in the records with new ones requested from the patient. Meanwhile, financial records should be placed on hold.

If the investigation determines that the problem is either an error or the result of medical identity theft, the patient should be notified and given appropriate information following the organization's mitigation procedures.

Notes

1. Ponemon Institute. "2013 Survey on Medical Identity Theft." September 2013. http://medidfraud.org/2013-survey-on-medical-identity-theft/.
2. Ibid.
3. Ponemon Institute. "Third Annual Survey on Medical Identity Theft." June 2012. http://www.ponemon.org/library/third-annual-survey-on-medical-identity-theft-ponemon-institute.

Joanne McNabb (Joanne.McNabb@doj.ca.gov) is the director of privacy education and policy at the California Attorney General's Office. Harry B. Rhodes (harry.rhodes@ahima.org) is a director of HIM practice excellence at AHIMA.

Article citation:
McNabb, Joanne; Rhodes, Harry B.. "Combating the Privacy Crime That Can KILL" *Journal of AHIMA* 85, no.4 (April 2014): 26-29.