Medical Identity Theft in the Emergency Department: Awareness is Crucial

Michelino Mancini, DO Lakeland Healthcare, Department of Emergency Medicine, St. Joseph, Michigan

Supervising Section Editor: Rick McPheeters, DO
Submission history: Submitted April 24, 2014; Revision received July 24, 2014; Accepted August 15, 2014
Electronically published September 24, 2014
Full text available through open access at http://escholarship.org/uc/uciem_westjem
DOI: 10.5811/westjem.2014.8.22438

Medical Identity theft in the emergency department (ED) can harm numerous individuals, and many frontline healthcare providers are unaware of this growing concern. The two cases described began as typical ED encounters until red flags were discovered upon validating the patient's identity. Educating all healthcare personnel within and outside the ED regarding the subtle signs of medical identity theft and implementing institutional policies to identify these criminals will discourage further fraudulent behavior. [West J Emerg Med. 2014;15(7):899–901.]

INTRODUCTION

The crime of medical identity theft is a growing concern in healthcare institutions. Medical identity theft is a practice in which someone uses another individual's identifying information, such as health insurance or social security number, without the individual's knowledge or permission, to obtain medical services or goods, or to obtain money by falsifying claims for medical services and falsifying medical records to support those claims.[1]

According to the Federal Trade Commission (FTC), medical identity theft accounted for 3% of identity theft crimes, or 249,000 of the estimated 8.3 million people who had their identities stolen in 2005.[2] More recently, the Ponemon Institute calculated that there were 1.84 million victims of medical identity theft in 2013.[3] These numbers were not specific to particular institutional departments, and emergency departments (EDs) may have a higher percentage of cases due to the growth in ED visits and the obligation to provide treatment in most emergency situations.

Numerous parties are negatively impacted by medical identity theft, including healthcare providers and payers. But, the stakeholder most adversely affected is the healthcare consumer. Consumers may receive inappropriate medications or treatment, which in some instances may be life-threatening. They can also suffer financial burdens when healthcare services provided to the medical identity thief are billed to the consumers or their insurance carriers.

The following cases illustrate common emergency medical encounters that were eventually exposed as incidents of medical identity theft. These incidents were discovered with the combined efforts of multiple healthcare associates, including registration clerks, nursing staff, security officers and physicians, and they were handled without compromising patient care or Emergency Medical Treatment and Labor Act (EMTALA) regulations.

CASE REPORTS

Case 1

An 18-year-old male presented to the ED with a chief complaint of a headache after a fall twelve hours prior. The patient reported that while walking down the last couple stairs in his house, he slipped and struck his head on the floor. Since the event he had experienced a persistent 6/10 sharp frontal headache. He denied any other associated symptoms including loss of consciousness, blurred vision, gait instability, neck pain, nausea, vomiting, or confusion.

The patient did not have a medical history and denied illicit drug or substance abuse. He answered all questions appropriately and had stable vital signs. His Glasgow Coma Scale was fifteen, and the remainder of his exam including neurological was negative. The patient was given hydrocodone/acetaminophen 5-325mg for his pain.

Upon reentering the patient's room to assess his pain, the attending physician encountered the patient being questioned by both the hospital security manager and a local police officer. The patient had presented to the ED without any personal identification cards and no means of validating his identity to the nursing staff or registration clerk. In addition, the security manager noted that his signatures on the hospital's standard financial agreement and

patient identification form did not match previous hospital-encounter signatures. The patient was later discharged from the institution uneventfully and without incarceration. Thirty days later, the information obtained by the hospital security manager and local police officer was used to successfully prosecute the patient for a felony of medical identity theft and insurance fraud.

Case 2

A 19-year-old female presented to the ED with mild lip swelling for two days. The patient denied any associated symptoms, including tongue swelling, shortness of breath, sore throat, voice change or difficulty swallowing. She denied taking any prescribed or over-the-counter medications. She also denied exposure to inhalants or skin irritants.

The patient did not have a medical history, and her vital signs were stable upon presentation. The physical exam was significant for mild lip edema without any tongue or oropharyngeal swelling. The remainder of the exam was negative. The patient was placed on a cardiac monitor and given intravenous diphenhydramine and methylprednisolone.

During her observational period, the registration clerk noted that the patient provided her a maternal insurance card and no personal identification cards. The clerk notified the security manager and, after further investigation, contacted the individual listed on the maternal insurance card. The card holder informed the security manager that she was not related to the patient and was concerned that her insurance card might have been stolen. After the complete resolution of her lip swelling, the patient was discharged and escorted to the local police department for further questioning. As a result of the information obtained by the registration clerk, security manager and local police department, along with the assistance of the victim, 60 days later the fraudulent patient was convicted of a felony for medical identity theft and insurance fraud.

DISCUSSION

In both cases described, the patients provided medical histories identical to their victims. The patient in the first case fraudulently used his brother's identification in order to remit costs of the ED visit to his brother's medical insurance. The patient's brother was found to be the victim and not an accessory to the crime. During the investigation of the second case, the patient was found to have two outstanding warrants for her arrest. These cases only illustrate a few motives for perpetrating medical identity theft. A telephone survey of chief compliance officers in acute healthcare facilities that had policies to counteract this crime revealed a belief that drug-seeking behavior and the presence of law enforcement officials in the ED may compel patients to commit medical identity theft to avoid potential arrest for other, unrelated crimes.[4] Whatever the underlying reason, this simple deceptive act can have significant negative effects on healthcare consumers, providers and payers.

The primary victim is usually an individual consumer (i.e., potential patient). Some individuals, including the disabled, minors, newborns, elderly and recently deceased, are even more susceptible targets for this type of theft. Medical identity theft may continue for years before it is discovered by a consumer who has a reason to scrutinize his or her medical bills or records. This fraudulent information can lead to denial of payments, exhausted health insurance and the inability of the consumer to obtain future health or life insurance. In addition to this financial burden, it may lead to life-threatening situations such as obtaining wrongful medications.

Medical identity theft is difficult to investigate and resolve. Some consumers believe that this crime is not a high priority due to the lack of laws addressing it and limited law enforcement resources. Medical privacy regulations including Health Insurance Portability and Accountability Act (HIPPA) do not address medical identity theft. In addition, this type of crime is treated differently than financial identity theft. The rights of victims of financial identity theft, such as the ability to see and correct credit report errors, obtain documents related to transactions involving their personal information and preventing consumer reporting agencies from reporting information that resulted from this theft, are not given to individuals of medical identity theft.[5] In most cases, victims cannot directly access their medical records and correct errors, and it is nearly impossible to prevent health care providers, medical clearinghouses or insurances from reporting misinformation.[1]

Healthcare providers and payers are usually the secondary victims of medical identity theft. Providers will likely write-off all healthcare expenses incurred as a result of treating fraudulent individuals.[6] Some speculate that ED losses can range from $750,000 to $3,000,000 annually from this theft, which directly affects an emergency medicine physician's compensation.[7] Providers and plans may unknowingly retain inaccurate information and share this information with third parties, such as life insurance carriers. With the proliferation of electronic health records, this information flows quickly and freely to numerous networks, further jeopardizing patient safety. Still unknown are the legal liability issues for healthcare providers and plans that may or may not have a process in place to prevent medical identity theft. In addition, common law is not yet clear on legal actions taken against a provider or plan related to negligence or malpractice with respect to medical identity theft.[6]

In 2008, the FTC issued regulations known as the Red Flag Rules, which required hospital institutions to develop and implement written identity theft prevention programs.[8] Congress later passed the Red Flag Clarification Act of 2010, which eased the requirements, thereby allowing many healthcare organizations to be exempt from this regulation. Consequently, many hospital institutions have

not instituted policies on medical identity theft or provided physician or non-physician staff the needed skills to counteract this type of fraud.

The Red Flag Rules enabled organizations to develop a program that includes four basic elements for responding to medical identity theft. The first is identifying relevant red flags within an institution's day-to-day operations, such as alerts from credit reporting companies, altered or other suspicious documents, mismatched personal identifying information (i.e., incorrect social security number with stated address), fraudulent credit account activity and notices from other sources (i.e., law enforcement). The second element is to detect these relevant red flags through verification and authentication methods. The next element is to prevent and mitigate identity theft. This would include notifying a supervisor or law enforcement in order to monitor and investigate current and existing accounts. Finally, the organization should maintain the program and remain up to date as identity theft tactics change and new technology, such as biometric software for iris scans and facial-recognition, becomes more readily available.

Recommendations

Medical identity theft is a complex crime, and a collaborative effort among individual victims, health information management technologists, institutional security officers, law enforcement, healthcare providers and payers is required to combat its effects. Developing an institutional policy that attempts to prevent and address complaints of medical identity theft must be a priority. In addition, broadening education of this crime to all healthcare associates including registration clerks, nurses and physicians is of great importance. Healthcare organizations that develop a reputation of thoroughly investigating and prosecuting medical identity theft will deter future attempts of this crime by fraudulent individuals. Finally, and most importantly, a heightened awareness of medical identity theft among all healthcare providers will help improve and maintain patient safety.

Address for Correspondence: Michelino Mancini, DO, Lakeland HealthCare, GME department, 1234 Napier Avenue, St. Joseph, MI 49085. Email: mmancini@lakelandregional.org.

Conflicts of Interest: By the *West*JEM article submission agreement, all authors are required to disclose all affiliations, funding sources and financial or management relationships that could be perceived as potential sources of bias. The authors disclosed none.

REFERENCES

1. Dixon P. Medical identity theft: The information crime that can kill you. World Privacy Forum Web site. Available at: http://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you. Accessed Apr 14, 2014.
2. Federal Trade Commission. FTC – 2006 Identity Theft Survey Report. Federal Trade Commission Web site. Available at: http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-2006-identity-theft-survey-report-prepared-commission-synovate/synovatereport.pdf. Accessed April 23, 2014.
3. Ponemon Institute, op. cit., 2013 Survey on Medical Identity Theft. Ponemon Institute Web site. Available at: http://medidfraud.org/2013-survey-on-medical-identity-theft. Accessed Apr 16, 2014.
4. Mancilla D, Moczygemba J. Exploring medical identity theft. *Prespect Health Inf Manag.* 2009;6(fall):1e.
5. Federal Trade Commission. Taking Charge: What to do if your identity is stolen. Federal Trade Commission Web site. Available at https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf. Accessed Apr 15, 2014.
6. Apgar C, Apple G, Ayers L, et al. Mitigating medical identity theft. *J AHIMA.* 2008;79(7):63–69.
7. Scorvo S. Patient identity fraud in the emergency department. Medpage Today's Kevin MD.com Web site. Available at: http://www.kevinmd.com/blog/2011/12/patient-identity-fraud-emergency-department.html. Accessed April 10, 2014.
8. Alexander J. Healthcare organizations must have an identity theft policy: FACTA or FICTION? *Healthc Financ Manage*. 2008;62(9):38-40.