Available Online at http://www.journalajst.com

ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ISSN: 0976-3376

Asian Journal of Science and Technology
Vol. 08, Issue, 11, pp.6746-6750, November, 2017

REVIEW ARTICLE

MEDICAL IDENTITY THEFT; A SYSTEMATIC REVIEW OF SOME SELECTED LITERATURES

[1]Sulaiman Bdamasi and *[2]Nasiru Sani

[1]Matma Plus Consult, Nigeria
[2]Research Scholar in Health Information and Management System, Department of Public Health and Community Medicine, Nims University Jaipur-303121, Rajasthan, India

ARTICLE INFO

Article History:
Received 13th August, 2017
Received in revised form
27th September, 2017
Accepted 26th October, 2017
Published online 30th November, 2017

Key words:
Medical identity theft,
Consequences of medical identity theft,
Medical identity fraud and
Negative impact on healthcare.

ABSTRACT

Medical identity theft is the fraudulent use of an individual's personally identifiable information (PII), such as name, social security number, and/or medical insurance identity number to obtain medical goods or services, or to fraudulently bill for medical goods or services using an unlawfully obtained medical identity. Unfortunately, the definition of medical identity theft (MIDT) and the consequences that are associated with the crime are not common knowledge to the general public. The study was a systematic review of some related literatures combined with life experience in order to bring forth a lasting measure of preventing medical identity theft Cases of identity theft are increasing, with incidents of identity theft rising more quickly (Cullen, 2007). Identity theft can be financial, medical, and character-related, with parents being the most common perpetrators.This study examined the experiences of medical identity theft victims using a phenomenological approach. The experiences of victim of medical identity theft are presented because of its financial, physical and emotional consequences that may result from this crime. A variety of negative emotions were experienced by the participants, including anger and fear. It was reviewed that Participants felt a lack of support from their families as well as law enforcement and other agencies from who help was expected. Medical identity theft can have a negative impact on reputation, consumers expect healthcare providers to be proactive in preventing and detecting medical identity theft. These trainings need to go beyond.A conclusion and recommendations were made which shows that 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.

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 (http://www. Worldprivacy forum.org/ 2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you). 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 (http://www.ftc.gov/sites/default/files/documents/reports/federal-trade- commission-2006-identity-theft-survey-report-prepared-commission-synovate/synovatereport.pdf).

Corresponding author: Nasiru Sani,
Research Scholar in Health Information and Management System, Department of Public Health and Community Medicine, Nims University Jaipur-303121, Rajasthan, India

Later, the Ponemon Institute calculated that there were 1.84 million victims of medical identity theft in 2013 (http:// medidfraud.org/2013-survey-on-medical-identity-theft). 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. Millions of Americans each year fall victim to identity theft. When identity theft involves healthcare, the consequences can be severe. It can result in losses to the healthcare provider from unpaid bills, the exhaustion of the victim's benefits, or even potentially life-threatening corruption of a patient's medical records. The crime also can play havoc with an innocent

consumer's credit rating. Medical identity theft may arise when a person seeks healthcare services or prescription of pharmaceuticals using someone else's name or insurance information. A recent nationwide survey conducted for the FTC found that 4.5 percent of the 8.3 million identity theft victims have experienced some form of medical identity theft. Last year, more than 113 million healthcare records were exposed or stolen as a result of healthcare data breaches. With so much healthcare data available it is no surprise that medical identity fraud is increasing. Medical identity fraud is now the fastest-growing type of identity fraud. Each year, more than two million individuals in the United States discover their medical data have been fraudulently used by cybercriminals and the problem is getting worse.

Medical identity fraud involves the use of personally identifiable information (PII) and protected health information (PHI) to fraudulently obtain medical services, healthcare devices, and prescription medications. False identities are also used for fraudulent healthcare billing. Medical identity theft can have a devastating impact on patients. Victims incur an average of $13,500 in out-of-pocket expenses after their identities have been stolen. Losses can be considerably higher. Medical identity fraud can go undetected for long periods of time and healthcare patients are not protected by the same legislation that protects them against credit card fraud. While the Fair Credit Billing Act limits losses to $50 for credit card fraud, victims are not protected from medical identity fraud. Patients may face a lifetime of financial hardship because of the misuse of their healthcare data. The impact on patients is not just financial. Medical identity fraud can have a negative impact on patient health. Victims may be denied medical services due to fraudulent use of their data, while the identity thief's medical treatment and medical history can become mixed up with the victim's electronic health records. According to the Medical Identity Fraud Alliance (MIFA), approximately 20% of victims of medical identity fraud have had an incorrect diagnosis and treatment or have experienced delays in receiving medical care as a result of fraudulent use of healthcare data. Medical identity fraud also has a negative impact on healthcare organizations and on the industry as a whole. There is growing distrust as a result of data breaches, while patients are now more apprehensive about sharing their data with healthcare providers. Patients are also more likely to switch providers because of data breaches and identity theft.
To raise awareness of the problem and to help healthcare organizations prevent medical identity theft and fraud, MIFA has released a new white paper to help healthcare organizations with their detection and mitigation efforts.

Ponemon Institute is presented the results of its fifth annual study on medical identity theft. This annual study is conducted to determine how pervasive this crime is in the United States, how it affects the lives of victims and what steps should be taken by consumers, healthcare providers and governments to stop its proliferation. Since last year's study, medical identity theft incidents increased 21.7 percent. In 2008, the Office of the National Coordinator (ONC) for Health Information Technology commissioned a study specifically addressing the privacy and security issues of health information exchange activities that may promote medical identity theft. The study summary noted the importance of appropriately implemented health information technology in preventing the occurrence of medical identity theft. Booz Allen Hamilton (2009) stated that the ONC study, along with a recent FTC regulation known as the Red Flags Rules, has significantly affected healthcare provider organizations, which are now required to develop and implement written identity theft prevention programs. (Alexander J *et al*., 2008) healthcare organizations now have a regulatory responsibility for addressing the issue of medical identity theft, though the methods used to prevent, detect, and remediate its occurrence are still unclear. The number of medical identity theft claims is rising; however, laws and regulations addressing financial identity theft are not generally inclusive of medical identity theft. Medical privacy regulations including the Health Insurance Portability and Accountability Act (HIPAA) do not address medical identity theft and in some cases pose barriers for victims of this crime theft victims. With the increasing use of electronic health records, privacy advocates fear an increase in medical identity theft. The use of e-health technology for providing medical services to remote areas will increase demands for stronger internal management practices to accurately establish patient identity before service is provided. Moreover, evidence suggests that healthcare employees and providers are frequently involved with committing or enabling medical identity theft by *San Diego Business Journal* (October 16, 2006). Medical identity theft occurs when someone uses an individual's name and personal identity to fraudulently receive medical services, prescription of drugs and/or goods, including attempts to commit fraudulent billing. In the context of this study, medical identity theft can also occur when an individual shares his or her health insurance credentials with others.

According to the research, sponsored by the Medical Identity Fraud Alliance (MIFA), medical identity theft is costly and complex to resolve. Because the crime can cause serious harm to its victims, it is critical for healthcare providers, health plans and technology/service providers to do more to help victims resolve the consequences of the theft and prevent future fraud. Government's increased influence and involvement in the delivery of healthcare services as a result of the Affordable Care Act (ACA) also requires it to become more proactive in addressing medical identity theft. Medical identity theft can suffer significant financial consequences. Sixty-five percent of medical identity theft victims in the study conducted by MIFA had to pay an average of $13,500 to resolve the crime. In some cases, they paid the healthcare provider, repaid the insurer for services obtained by the thief, or they engaged an identity service provider or legal counsel to help resolve the incident and prevent future fraud. Identity theft may be done by criminals, doctors, nurses, hospital employees, and increasingly, by highly sophisticated crimes. (Dixion, 2006). For many years, the top cause of lost or stolen patient data was a healthcare organization employee losing a device or having one stolen. (Shin, 2015) An employee may share patients' health data out of mischief. O'Brien reports, 2014suggests that, "A nurse at Albany Medical Centre is accused of stealing the identities of patients for at least a year and possibly as many as four. She and her boyfriend then used the information to set up credit card accounts and to print fake bank cheques." (databreaches.net, 2014). A survey conducted by the Ponemon Institute in 2014 suggests that 35 percent of medical Identity Thefts occurred as a result of family members using the victim's medical information. (Ponemon, 2014). In a nutshell, an insider, through whom personal medical records leak, can be a doctor, nurse, hospital employee or a family member. Therefore an insider data breach can be seen in two different

dimensions, i.e. within healthcare facilities, such as: healthcare providers and outside healthcare facilities, such as family and friends. The following paragraphs explain how MIDT can be prevented in reference to both dimensions: While medical identity theft and cyber securities breaches cannot be completely prevented, there are steps that both health services consumers and providers can take to slow its growth. Consumers should be informed about what they can do to prevent medical identity theft, including protecting their credentials from family and friends, monitoring their healthcare records and paying attention to insurance claims for possible signs their identity has been compromised. According to a study conducted by Ponemon (2014), Twenty-five percent of medical identity theft victims knowingly permitted a family member or friend to use their personal identification to obtain medical services and products and 24 percent say a member of the family took their credentials without their consent.

Another way of preventing MIDT from the consumer's side is multi-factor authentication. Crest faro *et al*, 2014, Multi-factor authentication has emerged as an alternative way to improve security by requiring the user to provide more than one authentication factor, as opposed to only a password. Authentication factors are usually of three kinds:

- **Knowledge:** something the user knows, e.g., a password
- **Possession**: something the user has, e.g., security token (also known as hardware token)
- **Inherence:** something the user is, e.g., a biometric characteristic.

To elucidate the above explanation, multi-factor authentication uses at least two different login credentials to verify a user; for example, requiring ta user to input biometric characteristics aside only password; using a password and a hardware token or sending some set of codes to the user's mobile phone, which will be required to be inputted during log in. All these are control measures that make unauthorized access more difficult. Prevention of medical identity theft within healthcare facilities can be achieved by intensifying organization's security in three ways, which are: managerial security, physical security and technical security.

Objectives

This study was intended to systematically review of some related literatures to prevent medical identity theft.

MATERIALS AND METHODS

This study was a systematic review of Medical identity theft practice, In our searches, we employed the following keywords and their combinations; literatures on medical identity theft (MIDT) and the consequences that are associated with the crime, Identity theft done by criminals, Medical identity theft corrupts medical record with erroneous information that can lead to incorrect diagnosis and treatments and is therefore, a quality-of-care issue that directly impacts the core mission of the healthcare industry, with the help of libraries, books, conference proceedings, data bank, and also search engines available at Google, Google scholar. Keywords, abstract, and full text. Technical reports were excluded since we focus on research papers.

Research Findings

A comprehensive literature search was conducted in the libraries, books, conference proceedings, data bank, Pub-Med, Medline, and Google Scholar reviewed. The available evidences indicated that;

Medical identity theft is costly to consumers: Unlike credit card fraud, 2 victims of medical identity theft can suffer significant financial consequences. Sixty-five percent of medical identity theft victims in our study had to pay an average of $13,500 to resolve the crime. In some cases, they paid the healthcare provider, repaid the insurer for services obtained by the thief, or they engaged an identity service provider or legal counsel to help resolve the incident and prevent future fraud.

Medical identity theft is a complicated crime to resolve: In the case of medical identity theft, the healthcare provider or insurer seldom informs the victim about the theft. Rather, on average, victims learn about the theft of their credentials more than three months following the crime and 30 percent do not know when they became a victim. Of those respondents (54 percent) who found an error in their Explanation of Benefits (EOB), about half did not know whom to report the claim to

Resolution of medical identity theft is time consuming to resolve: Due to HIPAA privacy regulations, victims of medical identity theft must be involved in the resolution of the crime. In many cases, victims struggle to reach resolution following a medical identity theft incident. In our research, only 10 percent of respondents report achieving a completely satisfactory conclusion of the incident. Consequently many respondents are at risk for further theft or errors in healthcare records that could jeopardize medical treatments and diagnosis. Those who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate. Finally, the impacted individual or a third party, such as the insurer or government agency paid the outstanding medical or insurance bills.

Medical identity theft can have a negative impact on reputation: Forty-five percent of respondents say medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions (89 percent of respondents). Nineteen percent of respondents believe the theft caused them to miss out on career opportunities. Three percent say it resulted in the loss of employment.

Consumers expect healthcare providers to be proactive in preventing and detecting medical identity theft: Although many respondents are not confident in the security practices of their healthcare provider, 79 percent of respondents say it is important for healthcare providers to ensure the privacy of their health records. Forty-eight percent say they would consider changing healthcare providers if their medical records were lost or stolen. If such a breach occurred, 40 percent say prompt notification by the organization responsible for safeguarding this information is important.

While medical identity theft cannot be completely prevented, there are steps both consumers and healthcare providers can take to slow its growth: Consumers should be informed about what they can do to prevent medical identity theft, including protecting their credentials from family and friends, monitoring their healthcare records and paying attention to insurance claims for possible signs their identity has been compromised. Twenty-five percent of medical identity theft victims in this study knowingly permitted a family member or friend to use their personal identification to obtain medical services and products and 24 percent say a member of the family took their credentials without their consent. Healthcare providers and government have a responsibility to ensure the security of the personal information they collect and to prevent unauthorized access to patient records. This is clearly a concern for respondents. Fifty-five percent of respondents say new regulations under the Affordable Care Act increase their chances of becoming a victim of medical identity theft.

In an intriguing case of identity theft, Martins Ugwu, a senior medical officer with Federal Ministry of Health, Abuja is discovered to have stolen the certificate with which he has worked for nearly a decade.

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 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 or pharyngeal 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. To sum it up the consequences for victims of medical identity fraud are much worse than for those of financial fraud. In a 2013 Ponemon Institute survey on medical identity theft, although only 36% of such victims incurred out-of-pocket costs, those that did paid out $19,000—far more than the $50 liability limit for fraudulent credit card charges. Victims whose profession requires them to pass medical tests can lose their jobs, and victims who are mothers and whose fraud is perpetrated by drug addicts could have their children taken away from them. The worst-case scenario for medical fraud victims is having their medical record contaminated by someone else's health information, such as an incorrect blood type or allergies. Even if the fraud is detected, the nightmare has only begun. It can be difficult for patients to flush mistaken information from the system because they don't know how many databases have their information and which ones need to be corrected.

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.

Conclusion

Medical Identity theft is a current global problem that causes lost in the amount of dollars, constant stress, and even threaten your life and health. Unless you check your medical records closely, you may discover you were defrauded only after the damage has been done.

REFERENCES

"Diagnosis: Medical Identity Theft." *Business Week*, January 8, 2007, 30.

Alexander J. 2008. "Healthcare Organizations Must Have an Identity Theft Policy: FACTA or FICTION?" Healthcare Financial Management. 62(9):38–40. [PubMed]

Alexander J. 2008. Healthcare organizations must have an identity theft policy: FACTA or FICTION? Healthc Financ Manage. 62(9):38–40. [PubMed]

Apgar, C., Apple, G., Ayers, L. *et al*. 2008. Mitigating medical identity theft. *J AHIMA.,* 79(7):63–69.[PubMed]

Data Breaches, "NY: Albany Medical Centre Nurse charged with stealing patient identities", available from https://www.databreaches.net/ny-albany-medical-center-nurse-charged-with-stealing-patient-identities/ obtained on 7th July, 2016

Deloitte Centre for Health Solutions, 2011. "Privacy and Security in Health Care: A fresh look".

Dixon P. Medical identity theft: The information crime that can kill you. World Privacy Forum Web site.[Accessed Apr 14, 2014]. Available at: http:// www. worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you.

Dixon P. Medical identity theft: The information crime that can kill you. World Privacy Forum Web site.[Accessed Apr 14, 2014]. Available at: http://www. Worldprivacy forum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you.

Dixon, P. "Medical Identity Theft: The Information Crime That Can Kill You."

Dixon, P. "Medical Identity Theft: The Information Crime That Can Kill You." 2014

Federal Trade Commission. FTC – 2006 Identity Theft Survey Report. Federal Trade Commission Web site. [Accessed April 23, 2014]. Available at:http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-2006-identity-theft-survey-report-prepared-commission-synovate/synovatereport.pdf.

Federal Trade Commission. FTC – 2006 Identity Theft Survey Report. Federal Trade Commission Web site. [Accessed April 23, 2014]. Available at: http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-2006-identity-theft-survey-report-prepared-commission-synovate/synovatereport.pdf.

Federal Trade Commission. Taking Charge: What to do if your identity is stolen. Federal Trade Commission Web site. [Accessed Apr 15, 2014]. Available at https:// www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

Kamala D. Harris, "Medical Identity Theft: Recommendations for the Age of Electronic Medical Records" October 2013.

Laura Shin, "Why medical identity theft is rising and how to protect yourself" May 2015. Obtained from http://www.forbes.com/sites/laurashin/2015/05/29/why-medical-identity-theft-is-rising-and-how-to-protect-yourself/#6400e440e200 on 4th July, 2016.

Mancilla D, Moczygemba J. Exploring medical identity theft. Prespect Health InfManag. 2009;6(fall):1e. [PMC free article] [PubMed]

Medical Identity Theft Final Report Prepared for the U.S. Department of Health and Human Services by Booz Allen Hamilton 2009. Contract number HHSP233200045008XI. Available at http://www.hhs.gov/healthit/documents/MedIdTheftReport011509.pdf (retrieved April 13, 2009).

Monegain, "Healthcare organisations at risk for more breaches" 2011, available from http://m. healthcareitnews.com/news/healthcare-organizations-risk-more-breaches Obtained on 20th September, 2017

Pam Dixion, "Medical Identity Theft –The information crime that can kill you", World Privacy Forum, May 2006.

Ponemon Institute, op. cit., 2013 Survey on Medical Identity Theft. Ponemon Institute Web site.[Accessed Apr 16, 2014]. Available at: http://medidfraud.org/2013-survey-on-medical-identity-theft.

Ponemon Institute, op. cit., 2013 Survey on Medical Identity Theft. Ponemon Institute Web site.[Accessed Apr 16, 2014]. Available at: http://medidfraud.org/2013-survey-on-medical-identity-theft.

Ponemon Institute, "Fifth Annual Study on Medical Identity Theft" February, 2015

Scorvo S. Patient identity fraud in the emergency department. Medpage Today's Kevin MD.com Web site. [Accessed April 10, 2014]. Available at: http://www. kevinmd.com/blog/2011/12/patient-identity-fraud-emergency-department.html.

Weeks, K. 2006. "Fast Growing Medical Identity Theft Has Lethal Consequences. *San Diego Business Journal* (October 16).

****