MEDICAL IDENTITY THEFT: A CYBERCRIME

by

Celenia Santos

A Capstone Project Submitted to the Faculty of

Utica College

April 2020

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Cybersecurity

Abstract

Medical identity theft has become a major issue in health care systems around the world, especially, with advancement in technology. While technology has been beneficial in improving service delivery and patient care in health care, it has also introduced numerous risks to patient safety. Cybersecurity issues have advanced with technology, thus increasing the rate at which medical identity thefts occur. The health care industry lags behind in curbing cybersecurity issues, and thus, it is vulnerable to many cyber-attacks. Numerous researchers have focused on the issue of medical identity theft because of its impact on patients, the health care sector, and the national economy. Possible solutions to the issue include training patients and health care practitioners on detecting and mitigating medical identity theft, the establishment of policies which promote protection of patients' data, legislative measures and creation of policies which re-assure patients the security of their information, as well as prioritizing medical identity theft as a key threat to patient safety.

Keywords: Patient Health Information, HIPAA, Cybercrime, Insurance, Fraud, Professor Paul Pantini, Cybersecurity, Computer Forensics.

Table of Contents

Medical Identity Theft: A Cybercrime

Statement of the Problem

Medical identity theft is an important area of concern for the health care sector because of the impact on patient care. Notably, the issue of medical identity theft has increased as a result of technology advancement in health care because of the Internet and the availability of computing devices (Mancilla & Moczygemba, 2009). Hence, this project addressed the problem of medical identity theft as a cybercrime in the health care sector.

This research aimed to examine medical identity theft as a cybercrime. The objectives of the study were to explore how medical identity theft occurs, to examine the role of technology in increasing the occurrence of medical identity theft, to assess the impact of medical identity theft in the health care sector, and to identify possible mitigation measures of medical identity theft. The research questions which guided this project are:

1. How has medical identity theft impacted patient care in the health care sector in the United States?
2. What role does the presence of more computing devices and the Internet have in increasing the occurrence of medical identity theft in the health care industry?
3. How can the training of health care providers and patients on the identification and prevention of medical identity theft help to mitigate its occurrence?
4. What role does the Health Insurance Portability and Accountability Act (HIPAA) have in influencing health care organizations and executives in the health care sector to work towards curbing medical identity theft in health care?

Having identified medical identity theft as a significant issue in health care, an analysis of the identified causes of the issue, the impact within health care, and the possible mitigation

measures are critical focus areas. These focus areas could serve as a basis for health care organizations and relevant state officials in the health care sector, to address and minimize its occurrence, as indicated in peer reviewed articles, scholarly journals, books, and related studies.

Mancilla & Moczygemba (2009) found that medical identity theft has become a major issue in the health care sector around the world. Health care organizations, patients, and health care officials have experienced the negative effects of medical identity theft and hence, it is necessary that the issue is prioritized in the health care sector and state laws. Advancement in technology has been beneficial to the health care industry by improving ways through which medical services are offered, including the storage of patient information. However, these advancements have made it easier for cybercriminals to commit medical identity theft, making the issue more difficult for health care organizations and law enforcement to curb. Medical identity theft poses risk similar to, or in some cases, more severe than those posed by other issues that interfere with patient care and quality service delivery and as such, it needs to be addressed.

Ponemon Institute (2015) defines medical identity theft as the use of one's social security numbers, personal information, and other confidential data to fraudulently acquire products such as prescriptions, drugs, and medical devices, as well as other medical services. This may involve the use of someone's health insurance information to receive health care services or reimbursement for medical services provided to a person not covered by the insurance policy. According to McNabb and Rhodes (2014), in most cases, medical identity theft is underreported in hospitals and when it is reported, it is categorized as health care fraud with little consideration of its impact on patient records and safety. As such, it is important to assess medical identity theft's significance in the health care sector, to a country's economy, and to patients' health and safety. McNabb & Rhodes (2014) cited a study from Ponemon Institute that found an estimated

1.84 million victims of medical identity fraud in 2013, which was a 21 percent increase from the previous year. This stipulated increase from the study by Ponemon Institute is in support of the view of Cassim (2015), stating that the rate at which technology in all sectors advances is almost the same rate with which identity theft crimes progress.

Notably, medical identity theft was first officially identified in 2006 by Pam Dixon in a major report, but the rate at which it has grown is alarming. Many health care organizations are still struggling with establishing the right strategies to prevent, identify and mitigate medical identity theft. Moreover, a larger part of medical identity theft occurs in hospitals, and as such, health care organizations need to maximize their efforts in curbing it (Dixon & Emmerson, 2017). Because of this observation, researchers have stated that the primary responsibility of dealing with medical identity theft lies with health care providers (McNabb & Rhodes, 2014). In addition to developing strategies to curb it, it is evident that health care organizations, the staff, patients, and state officials in the health care sector need to understand medical identity theft and effectively deal with it from the perspective of patient care. By handling the issue as a risk to patient care, medical identity theft may receive the attention it requires from health care providers, rather than when it is considered another case of fraud as is the norm in many health care organizations today (Ervural & Ervural, 2018).

How Medical Identity Theft Occurs

According to McNabb and Rhodes (2014), there are two ways that medical identity theft can occur. The first way involves an individual knowingly sharing his or her personal identifying information with another person, for instance, a friend or family member, so that the person can gain access to medical services or products. This form of identity theft is consensual and is more likely to occur when the larger part of the population is uninsured or underinsured. In such a

case, the insurance company is defrauded as it caters for medical expenses of individuals who are not its consumers.

In the second form of medical identity theft, patients' identifying information is accessed, shared or used by individuals who are unknown to the victim, which may include insiders in the health care industry (McNabb & Rhodes, 2014). staff from health care organizations may use patients' information to get reimbursement for medical procedures which were not done, or medical products which were not issued to the patient. It is also possible for cybercriminals to identify weaknesses in the IT system of a healthcare organization and gain access to patients' health information. As presented by Taitsman, Grimm, and Agrawal (2013), anyone who seeks and uses any health information that a patient has not chosen to share is committing medical identity theft, irrespective of their relationship to the patient or their responsibility at the health care organization.

Medical Identity Theft as a Form of Cybercrime

The origination and proliferation of medical identity theft correlates with the emergence of the digital revolution, a product of the influx in technology and technological development. As a product of such growth, cybercriminals began to and continue to have access to patients' medical information using computing devices and the plethora of resources available by and through the Internet. This new and unauthorized accessibility of other people's devices are nothing more than old crimes taking new form. This new form of crime, using computing devices and the Internet to hack into an individual's devices, networks, and other information storage platforms, is now referred to as cybercrime (Coventry & Branley-Bell, 2018).

The growth of electronic healthcare technology, such as electronic health records (EHR), telemedicine/telehealth, remote monitoring tools and the like, enable health care providers the

ability to maintain crucial patient information in digital form (Coventry & Branley-Bell, 2018). Consequently, the convenience this provides medical professionals directly burdens and threatens the individual whose information is being inputted, kept, and maintained on these digital platforms. This leads to the current situation where medical identity theft through cyber-attacks has become rampant.

According to Haider, Gates, Sengupta, and Qian (2019), there are numerous lessons to learn from the experiences that have taken place thus far regarding medical identity theft as a cybersecurity issue. For instance, the fact that medical identity theft was only officially identified in 2006 is alarming, considering that it may have been going on as soon as technology could support it. As such, the authors address the importance of learning from the past to come up with the best mitigation measures for today's risks, and to do so with a measured understanding of what people need in the future to mitigate medical identity theft. Therefore, it would be important for the health care industry to identify factors that incentivize or fail to dis-incentivize those choosing to engage in cybercrime in the health care sector today and use that knowledge to mitigate and prevent more harmful cases of medical identity theft in future.

Literature Review

The issue of medical identity theft has been addressed by numerous researchers because it impacts the health care sector across the world. According to Business Wire (2017), for every four United States (U.S.) consumers at least one has experienced a breach in their health care data as of 2017, with at least 50 percent of these victims experiencing medical identity theft as the security breach. As a result, medical identity theft is an area of concern for researchers of the health care industry, as well as other relevant parties such as security agencies. Moreover, the survey involving 2,000 U.S. consumers found that these breaches were more likely to happen in

hospitals, with the victims paying an average of $2,500 for every incident. This high occurrence in hospitals is attributed to the availability of important data, and the low defense mechanisms established by many health care organizations.

Taitsman, Grimm, and Agrawal (2013) referred to nearly 300,000 cases that the Centers for Medicare and Medicaid Services (CMS) handles on average annually, as well as the more than 77,000 complaints which the Office of Civil Rights received in 2012, related to medical identity theft, to show the extent of the issue. In the end, while not all 77,000 cases could be solved more than 18,000 corrective actions were undertaken. This is an indication that the parties responsible for investigating medical identity theft, such as CMS and law enforcement, are constantly dealing with the rising cases of medical identity theft, even though they do not manage to address most of the cases.

Financial Loss to Victims

Despite the efforts to correct medical identity theft cases, there is a high possibility that by the time corrective measures are undertaken the victims have already undergone financial losses and had their health put at risk. The risk to the patients' health comes from the false medical information history that appears on the victim's file that may result in them being treated for non-existent health conditions or denied necessary treatment in the future. Additionally, in the Ponemon Institute (2015) report, data from the annual survey of victims of medical identity theft indicates that the average cost of a data breach to patients whose information had been used to access medical services or for false claims from insurance companies, was $13,453 in 2014. As such, it is evident that victims of medical identity theft lose money when their information is used to cover other people's medical expenses. These statistics indicate that medical identity theft is an issue to be addressed with more vigor to protect patients and mend major gaps in the

healthcare sector in order to save on unnecessary costs and protect the health of individuals (Taitsman, Grimm, & Agrawal, 2013).

While researchers agree that cybercrime is also rampant in other industries, the issue on medical identity theft through cyber-attacks has been rising and the laxity in effectively curbing it remains a point of concern. As addressed by Coventry and Branley-Bell (2018), this is because efforts to curb cybersecurity issues in health care are not as evident as efforts made in other industries, making it easier for more cybercriminals to target the health care industry. As presented previously, in addition to having weak defenses, cybercriminals target the health care sector because it is a source of valuable data for a wide range of target populations.

Specifically, research indicates that patients' health records present cybercriminals with the opportunity to access a patient's personal information. This is dangerous because it could lead to other crimes such as robberies and kidnappings of the victims or their family members (McNabb & Rhodes, 2014). Over time, such issues and the threat posed by medical identity theft to patients have led health care providers and organizations to be blamed for doing very little to minimize cybercrime in health care (Coventry & Branley-Bell, 2018). Additionally, studies show that adoption of technology in the health care sector requires proper planning and implementation time, but this is not the case in many organizations which leaves health care organizations vulnerable to cyber threats (Kruse, Frederick, Jacobson & Monticone, 2017). As such, the health care industry remains under threat from cybercriminals due to the laxity in securing patient data that is gathered, stored, and updated in many healthcare settings.

Notably, the health care industry has implemented various strategies to improve patient safety but as research indicates, this may be part of the problem. Once an individual's medical

identity is stolen, no set framework exists for victims to correct the error (Federal Trade Commission, 2018).

Impact on Patient Care

According to McNabb and Rhodes (2014), when medical identity theft occurs it is capable of killing patients. This is because it can result in an improper diagnosis, in addition to harming a patient financially. Additionally, victims may be denied crucial medical services and goods because their records show that they may have accessed them, leading to their health and lives being endangered.

Armour (2015) addresses how medical identity theft has continued to leave people with expensive medical bills for services they did not receive. Taitsman, Grimm, and Agrawal (2013) presents that medical identity theft endangers patients and impacts quality of care. This view explains the new focus on medical identity theft and the push for health care providers, governments, patients and other policy makers to do more in curbing the issue. McNabb and Rhodes (2014) conducted an analysis of works by several researchers on the measures undertaken by the health care sector in curbing cybercrime and concluded that the health care industries continue to lag in curbing cybersecurity issues compared to other industries.

According to Taitsman, Grimm, and Agrawal (2013), patients experience financial losses when cybercriminals use their identity to obtain medical services using their insurance. This form of medical identity theft can be done in collaboration with fraudulent health care providers who have access to patients' information. In other instances, fraudulent health care providers use the stolen medical information to seek compensation from insurance companies for services that were not rendered to the patient. Cybercriminals at times will breach the security system of the

health care organization and steal patient health information, which is then used to claim medical services and goods.

McNabb and Rhodes (2014) also referred to some cases of medical identity theft in which the patients are co-conspirators with a third party with the intended result of defrauding the insurance company. In this scheme a patient will give out their personal information to friends or relatives who use it to receive medical products and services. In such a case, the patient being involved in the crime leaves the insurance companies as the victim of being defrauded. According to Coventry and Branley-Bell (2018), all forms of medical identity theft may negatively impact the health systems, reduce patients' trust in the health care organizations, and threaten human life because of the possible misdiagnoses that result from false information on the victims' health records. Cassim (2015) also posits that the financial losses suffered by victims of identity theft cause pain and suffering, damaged reputations, possible arrest from the crimes committed by the identity thief, and possible psychological damage to the victims.

The issue of whether technology advancement in health care has brought more benefits or challenges to the health care sector remains a contentious one. It is worth noting that technology advancement, and more so the Internet, has transformed the way the world operates and has impacted many industries positively and negatively. According to Cassim (2015), the Internet introduced cheap and instant communication around the world, making it easier for people to conduct business across a wide range of geographical locations. Ervural and Ervural (2018) also posits that the world continues to transform as a way of meeting today's complex and competitive demands in all industries, and this is achieved through application of relevant technology.

The Role of Technology

According to Haider, Gates, Sengupta, and Qian (2019), the health care industry has been undergoing a transformation through an influx of highly sophisticated devices, with little understanding of the involved risks. This is because of the growing complexity in medical conditions that require application of complex technology, irrespective of whether the medical personnel can correctly use it or not. Additionally, technology has enabled patient information to be stored, accessed and shared more conveniently through development of various mobile health applications (Kotz, Gunter, Kumar, & Weiner, 2017). In examining cybersecurity in health care, Coventry and Branley-Bell (2018) states that while technology has the potential of improving clinical outcomes and transforming health care delivery, concerns related to insecurity of health care devices and data are increasing. It is evident that increased connectivity to the Internet has created new cybersecurity vulnerabilities to medical devices and hence, medical data, which according to Haider et al. (2019), needs to be well-understood so that it can be addressed.

Notably, the Internet also brought cybercrime, which has become a major challenge for law enforcement. Haider et al. (2019) address that in spite of the benefits associated with technology, the need to integrate operational technology and informational technology has been a significant cause of cybersecurity issues because the application of technology is more effective when this integration occurs. As such, effective technology adoption requires proper implementation strategies and the right information technology personnel. Additionally, other forms of technology advancement such as the Internet of Things (IoT) have been major accelerators of the issue of cybercrime in all industries (Ervural & Ervural, 2018).

In the health care industry, cyber-attacks have been the highest forms of medical identity theft, as previously discussed. According to Cassim (2015), scholars have described identity theft

as the fastest growing white-collar crime, costing the U.S. economy more than $24.7 billion in 2012 and the British economy at least £1.3 billion annually as of 2015. Further associated, increased identity theft issues within new forms of communication technology expose vulnerabilities in computer networks and encourage criminals to breach them. Other types of technology embraced in health care, such as mobile health applications, have also resulted in more vulnerabilities for the health care sector and increased cases of medical identity theft (Asaddok & Ghazali, 2017).

Furthermore, researchers note that unlike in other cases of identity theft such as credit card fraud, where the thieves have limited opportunities to use the money, medical identity fraud victims take longer to realize that they have been victims of fraud (Mancilla & Moczygema, 2009). In the case of credit card fraud, it is possible for victims or the financial institution to easily identify the case of fraud and block the card. This limits major losses, and in the case any loss is experienced the victims are covered by insurance companies. However, medical identity theft victims sometimes only realize they have been defrauded when they are presented with expensive bills for medical procedures that they did not receive, or their insurance fails to cover them because they have exceeded the stated limit, even though they are aware that they have not reached their limit (Ponemon Institute, 2015). Therefore, researchers have found victims of medical identity theft as ones who experience the highest losses, in addition to the risk posed to their health as a result of these fraudulent activities.

The Role of Lawmakers

As McNabb and Rhodes (2014) presents how some important government policy makers are attempting to address this issue and ensuring the security of patients' personal health information. For instance, in 2013 California Attorney General Kamala D. Harris released a

publication termed Medical Identity Theft: Recommendations for the Age of Electronic Medical Records, which provides people with privacy protection.) The Attorney General stated that the health care industry needed to learn from other industries on effective methods of curbing medical identity theft. This is a valid sentiment because it has been established that health care organizations lag behind those in other industries regarding proper implementation of technology, and more so, dealing with cybersecurity issues in the industry (McNabb & Rhodes, 2014).

Additionally, as Cassim (2015) presents that the increase in medical identity cases led to the creation of the 1996 Health Insurance Portability and Accountability Act (HIPAA), which has regulated health care organizations and insurance companies to protect patient's information by complying with the stipulated rules in the Act. The impact of such legislative measures in curbing cybersecurity in health care is yet to be well-established, considering the issue of medical identity theft persists. Notably, Cascardo (2016) presents that the nature of the rules stipulated in HIPAA are complex and make it difficult for health care providers to comply, but because it is a legislative law, they have to find suitable means of complying. As such, it is important for health care organizations to create a plan that assists them in complying with the stated security rules and prioritizes the issue of medical identity theft.

Training Health Care Employees

Even as researchers highlight the possible solutions to cybercrime in health care, several scholars have considered the lack of proper training for health care providers and patients in handling personal health information as a contributing factor. McNabb and Rhodes (2014) address the important role played by consumers in identifying and reporting medical identity theft as a means of curbing the issue. However, there is an existing gap as it relates to timely

identification of medical fraud as many patients do not know they have been defrauded, until it is too late. McNabb and Rhodes (2014) write that the primary responsibility for addressing medical identity theft lies with the health care providers, who also need appropriate training so that they can create awareness of this issue in their organizations. Health care providers also need to implement an identity theft response plan, and appropriate policies and procedures to curb the issue. This can be achievable if health care organizations prioritize the issue and thus, see the need to create and implement policies for medical identity theft.

Specifically, McNabb and Rhodes (2014) advise that health care organizations should first train their staff members on appropriate use of technology. Then, staff should be trained on how to curb medical identity theft in case they come across it, thereby motivating health care organizations to take up a more active role in combating the issue. Moreover, McNabb and Rhodes (2014) present, that health information management personnel should grow awareness of medical identity theft by training registration and admitting staff on what to look out for in patient files and data management so that they can prevent cybercrime. The right IT personnel is critical in cybersecurity, as they can easily take part in preventing, identifying, and mitigating medical identity theft. IT personnel can identify loopholes that cybercriminals can use to access the valuable patient information stored within the record systems of healthcare facilities and inform others about them. IT personnel can help solution how this patient information can effectively be sealed to protect the privacy and security of patients.

Additionally, business and coding office staff should receive training on reporting medical record inconsistencies regarding patient history or treatment, as well as unusual billing patterns (McNabb & Rhodes, 2014). In the survey on victims of medical identity theft cited by Dixon and Emmerson (2017), half of the consumers who had experienced medical identity theft

found out about it on their own, identifying errors in their credit card statement when seeing charges that they did not make. Of the group that became aware of the medical identity theft, only one third of the consumers received an alert from the organization when the breach occurred. In the article, the author presents the importance of health care organizations establishing digital trust with patients to fight medical identity theft together, but this is only possible if proper training measures for both parties are put in place.

Furthermore, Dixon and Emmerson (2017) posited that in spite of medical identity theft occurring when patient information is under the care of healthcare providers, many patients have continued to trust their health care providers. Additionally, the survey, cited on victims of medical identity theft in the U.S., indicated that even as 88 percent of the consumers whose data was breached chose to trust their health care providers, there was a smaller percentage who mentioned their interest in being involved in securing their health care data. As such, healthcare organizations need to establish the right measures to improve internal defenses, strengthen cybersecurity capabilities, manage data breaches better and build resilience so that the consumers know their information is safe. This should happen across the healthcare sector in such a way that even as data is moved from one entry to the other, it remains protected.

Subsequently, issues of patients trusting their health care providers even after medical identity theft could be because patients do not know where else to go or how to establish if the health care organization was at fault. The study by Cifuentes, Beltrán, and Ramírez (2015), analyzing mobile health applications, presents that many mobile health applications are vulnerable. More importantly, the applications for communication and training health care providers were less vulnerable and can be used to deliver training on how to curb medical identity theft among health care providers as well as patients. This would help improve the trust

between patients and health care providers, as there would be fewer cases of cybercrime through medical identity theft.

In addition to training both medical staff and patients on how to identify and mitigate medical information theft, McNabb and Rhodes (2014) state that organizations should have a strategic plan for technology use and clearly defined procedures and policies showing individual staff responsibilities. McNabb and Rhodes (2014) further recommend that it would be important for someone from within and outside of the company to do regular compliance checks and audits. These efforts would detect and prevent inappropriate security breaches and inappropriate record access. Another recommendation is that health care organizations ought to be ready to investigate any suspicions raised by patients regarding medical identity theft and have a plan to rectify any information that may be found in the patient's record as a result of fraud.

According to the research conducted by Mancilla and Moczygema (2009), medical identity theft is rampant in the United States and that it is conducted by various individuals within and outside of the health care industry. Perpetrators include individual practitioners, health facilities, and cybercriminals. Medical identity theft leads to financial losses and causes greater risks associated with health outcomes due to inaccurate records and misdiagnosis of patients whose information has been stolen. These effects are quite paramount, which underscores the need to take the necessary measures to prevent them. These measures should involve all the stakeholders in healthcare provision and relevant security agencies in the government.

Discussion of the Findings

Technology and its Role in Medical Identity Theft

Benefits of technology in health care. Technology is an important component of the world today, as it has transformed the way all industries operate. According to Filkins et al. (2016), the rapid growth and incorporation of digital technologies into almost every aspect of today's life creates extraordinary opportunities for people in all industries. In the healthcare industry, technology has changed how medical services are offered, in addition to improving the communication and informatics sectors of the industry. As such, technology remains a crucial part of the health care industry. Coventry and Branley-Bell (2018) state it has a high potential in the improvement of clinical outcomes and transformation of care delivery.

For instance, technology has helped reduce many issues in the industry such as healthcare organizations successfully incorporating technology into daily operations, effectively minimizing manual work expected to be done by health care providers therefore enabling them to serve more patients and retain the staff. As such, delivery of medical services has become more efficient because of the incorporation of technology into the health care sector.

According to Cifuentes, Beltrán, & Ramírez (2015), technological advancement has also led to the invention of mobile health applications, which has significantly changed how patients and medical personnel relate. Using the mobile health applications, healthcare providers can easily diagnose diseases as well as undertake possible preventive or curative measures as suggested through the applications. Additionally, both patients and healthcare providers can access any information they want at any time through these applications because they are connected through the Internet. Other important applications of technology in health care include

the use of advanced equipment to offer critical care to patients, thereby reducing the mortality cases compared to the pre-technology era.

Burns and Johnson (2015) further examine the role of technology in storing and sharing health information and this is supported by the transformation that has been experienced in the health informatics sector through the use of electronic health records (EHR). Technology has also changed medical research as it enabled researchers to identify causative factors of strange diseases and how to treat them, in addition to coming up with improved ways of treating existing diseases or conditions.

Challenges brought by technology advancement. Even as technology advancement is associated with positive changes in the health care, as discussed above, many researchers have addressed numerous challenges that have resulted from it. For instance, Cassim (2015) presents that the introduction of the Internet brought various risks and dangers, making networks and devices vulnerable to cyber-attacks. Cifuentes, Beltrán, and Ramírez (2015) also address the increased possibilities and cases of cyber-attacks in devices used for mobile health applications. As such researchers present, the fast rate at which technology is advancing is also the rate at which cybercrime advances. For a sector such as health care, advancement in cybercrime is a crucial issue because it puts at risks patient care and human life.

Medical Identity Theft in Comparison to Other Forms of Identity Theft. Cassim (2015) presents cases of identity theft have continued to increase with advancement in technology. As discussed, medical identity theft differs from other forms of identity thefts because of the impact the former has on its victims, health care organizations and national economies. Therefore, while victims of other identity theft cases only face the risk of experiencing financial losses, victims of medical identity theft have their health and lives at risk

because of the misdiagnoses that may occur when one uses their health information fraudulently. This is in addition to the failure to be

covered by one's insurance policy when they need it after being a victim of medical identity theft. In the case of other identity thefts, the victim is reimbursed for any loss. Meanwhile in medical identity theft, the victims cater for the losses (Ponemon Institute, 2015).

Additionally, as presented by Ervural and Ervural (2018), many organizations consider cybersecurity as a technology issue and as such, they address it with the perceived necessary technical knowhow. However, health care organizations consider cases of medical identity theft as any other fraud case and therefore impacts the rate at which they employ measures to curb it. This response to identity theft in health care organizations and those in other industries also differentiates medical identity theft from other kinds of identity thefts. Other sectors are more prepared to identify, prevent, and mitigate identity theft compared to the health care sector. For instance, as Ponemon Institute (2015) asserted, other identity thefts, such as credit card thefts, are easily identified and stopped before they can cause significant damage. Additionally, while one is compensated if they become victims of other forms of identity theft, in medical identity theft, the victim experiences more issues during resolution, on top of being defrauded, as he or she has to pay for any medical bills resulting from the theft and in some cases, they miss out on being covered by their insurance companies even when they need medical services or products.

Causes of Medical Identity Theft. One cause of medical identity theft is the in curbing the issue. It is worth noting that while the benefits and challenges of technology advancement have been experienced across all the industries, the health care sector has been marked as one that lags behind in proper planning and implementation of technology, as well as curbing cybersecurity issues. According to Coventry and Branley-Bell (2018), one of the reasons why

cybercriminals target health care is because they have noted that it has weak defenses. This is because, as earlier stated, many health care organizations do not put in as much effort as organizations in other sectors to identify, prevent and mitigate cyber-attacks.

Another important cause of medical identity theft is the lack of proper training for medical personnel and patients regarding how to prevent, identify and mitigate the issue. As McNabb and Rhodes (2014) asserted, many health care providers lack the necessary skills to curb medical identity theft. This is because many of the people who work in health care organizations are only qualified for their specific role, with little or no background in information technology (IT). For instance, the expertise of nurses and doctors revolves around offering medical services, irrespective of the complex nature of the technology they use in their daily duties. As such, the lack of the necessary knowledge and skills regarding cybersecurity puts the health care organization at a risk of being cyber-attacked.

Additionally, the nature of work of health care organizations may be a contributing factor to the laxity in dealing with medical identity theft compared to organizations in other industries. This is because health care organizations are mostly focused on delivering medical services, and as such, many health care professionals may believe that paying attention to cybersecurity is not their main objective. Moreover, many health care providers are overworked from performing their medical duties and therefore may lack the time and energy to focus on medical identity theft.

Patients. Many patients lack the correct knowledge of when their medical identity is at the risk of being stolen, as well as how to avoid it and deal with the theft when it occurs. In the survey on victims of medical identity theft referred to by Dixon and Emmerson (2017), it was evident that many patients take a long time to realize that their medical identity was stolen,

putting their health at more risk as they might only notice when it is too late. In addition, many patients do not know what to do after they have discovered fraudulent actions, with many of them going back to seek advice from their health care providers because of the trust these patients have in them. Notably, this is dangerous because some personnel in the health care organization may have been involved in stealing and using the patient's information, and hence, the victim's issue may not be well-addressed.

In addition to the patients' lack of proper knowledge regarding medical identity theft, patients lack information regarding the impact this kind of cybercrime can have on their health. For instance, in the case of those patients who voluntarily offer their information to other people and defraud insurance companies, the patients fail to realize that their health records will be affected as they will have the other person's information, and that this could be detrimental to their health. Other crucial information such patients lack is that their insurance policy could fail to cover them in case of an emergency because they may have exhausted the stated limit.

Professional and ethical standards. Lack of proper professional and personal ethical standards on the part of hospital organizations also contributes to identity theft. While health care providers are required to comply by laws such as HIPAA and must protect patient information, some institutions and individuals fail to uphold the necessary ethical standards and comply with such rules. Researchers such as Cascardo (2016) addressed the challenges facing compliance with regulations such as HIPAA, stating that many individuals and organizations make lesser efforts in complying, and end up exposing patient information to cybercriminals. This lack of adherence to the stated laws and ethical standards result in the misuse of patient health information by some health care providers. Moreover, some of the health care workers are

actively involved in these acts of medical identity theft as a way to make more money, thus making them cybercriminals as well.

State and Federal Government. Failure by some governments and top health care executives to develop effective mechanisms to curb medical identity theft is also a contributing factor to its spread. Taking the example of the U.S., which has established laws such as HIPAA to guard patients' privacy, it is important to note that the creation of such laws alone is not enough to curb the issue (Cascardo, 2016). This is because, as stated earlier, the issue of medical identity theft was officially made public as recently as 2006, while HIPAA had been in place for at least ten years at the time. As such, the existence of HIPAA did not hinder the prevalence of cyber insecurity in the health care industry and as of today, one would be justified to state that it is not enough unless integrated with other measures. Therefore, there is an existing gap between cybercrime in health care, and the development of effective measures to curb it.

No limit computing devices. The lack of proper limits around the use of computing devices and the Internet has also contributed to the rising cases of cyber insecurity in health care. According to Burns and Johnson (2015), computing devices and ubiquitous networks have increased the rate at which patients and health care practitioners engage and share health information. However, in spite of the notion that many governments control how people use the Internet and computing devices, it is evident that this has not succeeded in restricting people and reducing cybercrime. Thus, technology advancement in health care has also increased vulnerabilities to cyber-attacks because of the failed attempts to restrict people's use of networks.

Impact of Medical Identity Theft as a Cybercrime in Health Care. Medical identity theft through cyber-attacks continues to pose a major safety threat to patients and the health care system. Interfering with hospital systems leads to loss of important patient information such as

that found in EHRs, thus, endangering the health and life of patients whose information is lost. Additionally, the issue of stealing health information from hospital systems has been associated with reduced patient trust in the system, and therefore interferes with patient's health care procedures, as they are sometimes forced to look for a new health care provider.

Medical identity theft causes massive financial losses to patients, as they have to resolve for the medical services or goods offered to the thief. According to Dixon and Emmerson (2017), at least 50 percent of those who experienced a breach in their security information in the survey conducted among 2,000 U.S. consumers had to pay $2,500 for every incident. This is an indication of how financially harmful medical identity theft can be to a patient. Further, the financial losses may have more implications to the life of a patient, such as failing to meet other financial obligations including paying rent or mortgage, school fees, buying food and more. Consequently, patients who experience financial losses from these fraudulent acts may end up suffering from stress-related conditions and diseases, which affects their health and endangers their lives.

In addition to the risk of getting stress-related diseases, cybercriminals also endanger the health and life of patients through the omission or addition of crucial health information that may interfere with treatment of the patient. Taitsman, Grimm, and Agrawal (2013) stated examples of incidents in which patients are wrongly labelled as diabetic or HIV-positive when people with the stated conditions use their medical identity to obtain services. In other instances, patients are denied medical services which are legitimate, such as a pharmaceutical prescription or the failure to be issued supplies such as wheelchairs, because the medical records show that the patient already received it. Such issues are life threatening to patients and also put the credibility of the health care system to question. It is also worth noting that medical identity theft may cause

patients to be denied financial reimbursement from their insurance companies as they are considered to have exhausted the service limits. As such, whether the medical identity theft is consensual or from a stranger, it risks the health and life of patients.

Another significance of medical identity theft comes from the impact on the economy of a country. According to Cassim (2015), the general cost of identity theft on the U.S. economy in 2012 was nearly $24.7 billion, while the British economy was stated to lose at least £1.3 billion annually. Such statistics are an indication that medical identity theft interferes with the economy of a country and therefore hindering delivery of other important services. Governments also have to incur costs and resources in establishing legislations to curb cybercrime in health care. Such measures require time, money and human capital which can all be utilized elsewhere if these cybercriminals were non-existent. Insurance companies also experience massive financial losses as they reimburse people who are not their clients or pay for medical procedures and goods which were not rendered.

Possible Solutions to Medical Identity Theft. One important way of curbing medical identity theft through cyber-attacks is by training health care providers on the appropriate measures to use in identifying, preventing and mitigating such attacks. As Burns and Johnson (2015) asserted, the application and integration of IT in health care requires a cautious approach so that it can protect the security of patients' health information. Kruse et al. (2017) also stated that before adopting technology in health care, it is important to create a plan and the right implementation strategies to curb vulnerability to modern trends and threats. As pointed out by these researchers, being well prepared to adopt and implement any technology in a health care organization requires more than just acquiring it. Proper preparation techniques for these

organizations entails training staff members on how to minimize cyber-attacks through timely identification, as well as what to do if an attack has successfully occurred.

According to McNabb and Rhodes (2014), it is up to the health care providers to create awareness of medical identity theft, which can only be successfully achieved if the staff members are well-trained to deal with the issue. According to Filkins et al. (2016), cyber situational awareness in any health care organization is crucial to combating any cyber-attacks, even from highly organized criminals. As such, health care professionals ought to act as leaders in curbing the issue by ensuring that they create proper awareness across the whole organization. For instance, admitting and registration staff should be well-trained on how to take note of any suspicious practices and patterns and know how to handle them before they turn into identity theft cases. Such suspicious behavior could include a patient who states their insurance number but fails to produce an insurance card. In addition, the staff involved in coding and other business operations in the organization should be trained to report any inconsistencies regarding the patient's history or treatment, as well as any unusual billing patterns.

While focusing on training the medical practitioners and staff of health care organizations, it is important to use the appropriate strategies to ensure effectiveness of the trainings. For instance, McNabb and Rhodes (2014) suggest that training should be centered around the impact of medical identity threats, especially on the main victims, the patients. This would encourage the health care organization staff members to work towards protecting patients' health information as much as they can, while avoiding being engaged in unethical and criminal practices that promote medical identity theft. Additionally, focusing the training on the impact of these breaches on the health care organization may also encourage those who are loyal and

committed to their organizations to engage in prevention measures against cybercrime in their workplace.

Once health care providers are well-trained on the issue of medical identity theft, they can take part in training patients and creating more awareness on the matter. For instance, health information management professionals should be on the forefront of creating awareness and training patients on the importance of protecting their health information. Additionally, patients should be trained on how to identify threats to their personal health information, as well as mitigation measures once any attack occurs. For patients who voluntarily issue personal health information to others, they should be trained on the risks which arise from such actions in terms of their health, as well as possible lawsuits in case they are caught.

Another important aspect a patient should be trained on is how to choose a reliable health care provider by identifying organizations which are known to have a history of failing to protect their patients' information. With such information, patients would avoid being blinded by trust in their health care organizations even after their information has been breached (Accenture, 2017). Therefore, with the right training, patients would know the extent to which their health care provider goes to protect their health information, as well as if and when they are involved in medical identity theft. Filkins et al. (2016) also stated that when people are well-trained on responsibility and equipped with the right cyber literacy, they can understand their role as data owners, and this would help them to guard their data well. This is applicable to patients regarding the need for them to do everything possible to ensure the safety of their information.

The health care organization should also have policies and procedures in place to prevent, detect, and mitigate medical identity theft. This is because training the staff without having procedures and policies in place would be ineffective in curbing the issue. Once proper policies

and procedures are established, the staff can understand and implement them, and the training programs on medical identity theft could also be tailored to them (McNabb & Rhodes, 2014). Notably, institutions should have ways of enforcing these company policies on security to deter any staff member from breaching them, thus creating a culture that embraces and prioritizes the security of patient health information.

Additionally, health care organizations should invest in the right form of IT equipment and personnel to ensure that vulnerability to cyber-attacks on their systems is minimized and patient health information is safe. As Cassim (2015) stated, adoption of technology in health care organizations also entails investing in the right type of technology. As such, the type of technology in a health care organization should involve the right IT personnel who can also ensure that they create a health safety identifier unique to the organization. Having effective IT personnel also helps to ensure that all the systems of the organization are well linked and are synchronized to provide maximum security against cyber threats. It is also important for the health organizations to be wary of what systems they for data storage so that their system is not exposed to cyber-attacks, such as using a cloud system.

Another important way to curb medical theft identity is to make cybersecurity an integral part of patient care and safety. As Coventry and Branley-Bell (2018) posited, the first step in addressing cybersecurity issues in health care is identifying its importance in patient care. Thus, it should be prioritized together with other measures to ensure patient safety, such as having the right response systems to patients' needs and having safety policies in organizations. Notably, many health care organizations have been cited to have laxity in curbing medical identity theft issues and hence, incorporating it in patient safety measures would ensure that it is made a

priority. This view is important considering the danger that medical identity theft poses to patients' health and their lives.

Subsequently, another effective measure in curbing medical identity theft is to create regulations and legislations for health care organizations to comply with in protecting patient health information. This is an important measure for governments to take so that they can play a role in protecting the security of patients' health information. For instance, the legislative law known as HIPAA, enacted in 1996 in the U.S., is meant to ensure that health care organizations do not breach their patients' information. In spite of the challenges experienced in complying with HIPAA as cited by Cascardo (2016), health care organizations need to ensure that they create a plan to ensure compliance. For instance, the organizations can find the right person or team to lead it in compliance procedures, and this would increase the chances that they are adhering to the stipulated laws.

Additionally, as the government has developed laws such as HIPAA to ensure protection of patients' information, they also need to develop more effective measures to prevent and curb medical identity theft. In the case of health care organizations, they are guided by HIPAA laws to protect patients' health information. Still, the issue prevails because the laws meant to control cybercriminals are not effective enough to stop them from committing medical identity theft. As such, law enforcement needs to create, as well as implement, better and more effective strategies to prevent cybercrime in health care. More importantly, the legislative measures applied by law enforcement against medical identity theft should be specific to health care rather than being categorized under other forms of identity theft. This because other forms of identity theft such as those involving credit cards do not directly impact patient safety, as in the case of medical identity theft.

Conclusion

The objectives of the study which included exploring how medical identity theft occurs, examining the role of technology in increasing the occurrence of medical identity theft, assessing the impact of medical identity theft in the health care industry, and identifying possible mitigation measures of medical identity theft, were met. The study established that the occurrence of medical identity theft has been fueled by advancement in technology in the health care sector and other industries, and the failure to identify it as an issue related to patient safety. The possible mitigation measures identified included training health care practitioners and patients on how best they can detect, prevent, and mitigate medical identity theft by focusing on cybersecurity. Notably, as stated in the rationale of the study, an analysis of the findings of the project would be useful as a basis for health care organizations and governments to establish measures for curbing medical identity theft and reducing its impact on patient care.

The study also addressed the research questions established for the study, and the findings indicated the following: Medical identity theft has caused negative outcomes in patient care in the U.S. through various means including: misdiagnoses, which may result from the existence of another person's information on the patient's medical file, inaccessibility to benefits from insurance policies because of exhausted limits by the fraudsters, and possible stress-related complications in patients because of the financial losses incurred from the theft incidences; The existence of more computing devices and the Internet in health care have provided an easier platform for cybercriminals to access medical information of patients and share or use it for their benefit; Training of health care providers and patients to identify and prevent medical identity theft helps to minimize its occurrence by offering them with the relevant information to catch possible fraud cases in a timely manner, as well as to know what to do if they identify or suspect

a possible case of medical identity theft. It also helps patients and health care providers to realize the impact of medical identity theft on patient care, and work towards curbing it; and, HIPAA laws influence health care organizations and executives in the health care sector to protect patients' health information or face legislative measures. Thus, HIPAA compels many health care organizations to establish effective measures to ensure they protect patients' health information to avoid being legally implicated.

References

Armour, S. (2015, August). How Identity Theft Sticks You With Hospital Bills. Retrieved from https://www.wsj.com/articles/how-identity-theft-sticks-you-with-hospital-bills-1438966007

Asaddok, N., & Ghazali, M. (2017). Exploring the usability, security and privacy taxonomy for mobile health applications. In International Conference on Research and Innovation in Information Systems (ICRIIS), 1-6.

Burns, A. J., & Johnson, M. E. (2015). Securing health information. IT Professional, 17(1), 23-29.

Cascardo, D. (2016). Compliance challenges facing healthcare providers in 2016. The Journal of Medical Practice Management, 31(5), 276-279.

Cassim, F. (2015). Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves? Potchefstroom Electronic Law Journal, 18(2), 68.

Cifuentes, Y., Beltrán, L., & Ramírez, L. (2015). Analysis of security vulnerabilities for mobile health applications. International Scholarly and Scientific Research & Innovation, 9(9), 1067-1072.

Coventry, L., & Branley-Bell, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48-52.

Dennis, M. A. (2019, September). Identity theft and invasion of privacy. Retrieved from https://www.britannica.com/topic/cybercrime/Identity-theft-and-invasion-of-privacy.

Dixon, P., & Emmerson, J. (2017, December). One in Four US Consumers Have Had Their Healthcare Data Breached, Accenture Survey Reveals. Retrieved from https://newsroom.accenture.com/subjects/technology/one-in-four-us-consumers-have-had-their-healthcare-data-breached-accenture-survey-reveals.htm

Els, F., & Cilliers, L. (2017). Improving the information security of personal electronic health records to protect a patient's health information. Conference on Information Communication Technology and Society (ICTAS), Umhlanga, South Africa.

Ervural, B. C., & Ervural, B. (2018). Overview of cyber security in the industry 4.0 era. In Industry 4.0: Managing the digital transformation (pp. 267-284). Springer, Champ.

Federal Trade Commission. (2018, September). Medical Identity Theft. Retrieved from https://www.consumer.ftc.gov/articles/0171-medical-identity-theft

Filkins, B. L., Kim, J. Y., Roberts, B., Armstrong, W., Miller, M. A., Hultner, M. L., ... & Steinhubl, S. R. (2016). Privacy and security in the era of digital health: What should translational researchers know and do about it? American Journal of Translational Research, 8(3), 1560.

Haider, N., Gates, C., Sengupta, V., & Qian, S. (2019). Cybersecurity of medical devices: Past, present, and future. In T. Deer, J. Pope, T. Lamer, & D. Provenzano (Eds.), Deer's Treatment of Pain (pp. 811-820).

Kolata, G. (2011, October). Sports Medicine Said to Overuse M.R.I.'s. Retrieved from https://www.nytimes.com/2011/10/29/health/mris-often-overused-often-mislead-doctors-warn.html

Kotz, D., Gunter, C., Kumar, S., & Weiner, J. (2017). Privacy and security in mobile health: A research agenda. Computer, 49(6), 151-177.

Kruse, C., Frederick, B., Jacobson, T., & Monticone, K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25, 1–10.

Mancilla, D., & Moczygemba, J. (2009). Exploring medical identity theft. Perspectives in health information management/AHIMA, American Health Information Management Association, 6(Fall).

McNabb, J. & Rhodes, H. B. (2014). Combating the privacy crime that can kill. Journal of The American Health Information Management Association (AHIMA), 8(4), 26-29.

New FTC statistics affirm World Privacy Forum's 2006 Medical Identity Theft report; give first robust medical identity theft statistics. (n.d.). Retrieved 2006, from https://www.worldprivacyforum.org/2007/11/blog-new-ftc-statistics-affirm-world-privacy-forums-2006-medical-identity-theft-report-give-first-robust-medical-identity-theft-statistics/

Ponemon Institute (2015). Fifth annual study on medical identity theft. Ponemon Institute Research Report. Retrieved 2015, from http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

Taitsman, J. K., Grimm, C. M., & Agrawal, S. (2013). Protecting patient privacy and data security. The New England Journal of Medicine, 368, 977-979.