2018

Strategies to Prevent and Reduce Medical Identity Theft Resulting in Medical Fraud

Junior V. Clement
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Junior V. Clement

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Jamie Patterson, Committee Chairperson, Doctor of Business Administration Faculty

Dr. James Glenn, Committee Member, Doctor of Business Administration Faculty

Dr. Judith Blando, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2018

Abstract

Strategies to Prevent and Reduce Medical Identity Theft Resulting in Medical Fraud

by

Junior Vibert Clement

MSA, Central Michigan University, 1992

BS, University of Maryland University College, 1990

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

February 2018

Abstract

Medical identity fraud is a byproduct of identity theft; it enables imposters to procure medical treatment, thus defrauding patients, insurers, and government programs through forged prescriptions, falsified medical records, and misuse of victim's health insurance. In 2014, for example, the United States Government lost $14.1 billion in improper payments. The purpose of this multiple case study, grounded by the Health Insurance Portability and Accountability Act as the conceptual framework, was to explore the strategies 5 healthcare leaders used to prevent identity theft and medical identity fraud and thus improve business performance in the state of New York. Data were collected using telephone interviews and open-ended questions. The data were analyzed using Yin's 5 step process. Based on data analysis, 5 themes emerged including: training and education (resulting to subthemes: train employees, train patients, and educate consumers), technology (which focused on Kiosk, cloud, off-site storage ending with encryption), protective measures, safeguarding personally identifiable information, and insurance. Recommendations calls for leaders of large, medium, and small healthcare organizations and other industries to educate employees and victims of identity theft because the problems resulting from fraud travel beyond the borders of medical facilities: they flow right into consumers' residences. Findings from this study may contribute to social change through improved healthcare services and reduced medical costs, leading to more affordable healthcare.

Strategies to Prevent and Reduce Medical Identity Theft Resulting in Medical Fraud

by

Junior V. Clement

MSA, Central Michigan University, 1992

BS, University of Maryland University College, 1990

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

February 2018

Dedication

Thank God for guiding and providing me with the wisdom to successfully complete this doctoral dissertation project. Subsequently, I dedicated this doctoral project to Merle M. Clement, my wife, and friend for the past 14 years. Merle stood by my side when times were good or bad and continued to encourage and supported me during tough periods. I also dedicated this manuscript to Allison L. King, my mother, and friend for always sticking by my side despite the situation. I also shared special thanks and appreciation to Lemuel King, my dad, and friend for being there for my mom and the family. Finally, I also extended my dedication to Alicia L. Clement, my daughter, and friend for reconnecting back into my life. Without-a-doubt, her return into my life after 10 years was justly a special gift from God! Without question, the three women mentioned above are truly a blessing in my life!

Acknowledgments

Special thanks to Dr. Jamie Patterson for her unwavering support during tough periods of this collegiate dissertation. During tough moments involving major delays, I considered quitting completion of the doctoral project, but Dr. Patterson's positivity and contagious it-can-be-done attitude was the driving force that played a pivotal role in regaining confidence and continued the quest! I also extended thanks to Dr. James Glenn for his involvement as Second Committee Member for sharing his expertise and expedited turnarounds that played a key role during completion of this project. I also highly appreciated Dr. Judith Blando as University Research Review and Dr. Karlyn Barilovits as Program Director for their constructive feedbacks that made a difference towards the end result of this project. Without the guidance and support of the four-person collaborative team mentioned above, I would not have been successful in completing this all-important dissertation project!

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Healthcare-related fraud in hospitals usually occurs by way of providers' deception, identity theft or "insider job" committed by employees (Amigorena, 2014; Luizzo & Scaglione, 2014; Wang, Gupta, & Rao, 2015) leading to medical identity fraud. Federal Bureau Investigation (FBI) officials' defined fraud as a deception for personal gain; it results in needless costs that are inconsistent with accepted norms (Dube, 2011). McNabb and Rhodes (2014) argued that thieves can victimize someone without their knowledge. The financial losses from healthcare fraud cost $70 to $236 billion annually that ranged from 3% to 10% as stated by (Luizzo & Scaglione, 2014). Federal Trade Commission (FTC) officials stated that identity theft accounted for 16% of 29% of fraud complaints in 2015 that affected business profits (FTC, 2016). Due to the rampant increase of fraud, business leaders need to implement effective strategies in their organizations to combat fraud (Selamat & Babatunde, 2014) and identity theft. I explored the strategies healthcare leaders use to reduce medical identity fraud and thus improve business performance.

Background of the Problem

Medical identity fraud claimed 2.3 million victims in 2014 and resulted in out-of-pocket expenses totaling $13,500 per person for a combined total of $20 billion (Votta, 2016). The rampant effects of identity theft raised major concerns as the financial losses from medical identity theft totaled $36 billion yearly (Martin, Borah, & Palmatier, 2017) and government officials need to impose stiffer penalties. Testimony from Votta (2016) stated that stolen funds per physician average $1.4 million. Votta warned that there was a

high-demand on the black market for protected health information (PHI), a demand that increased from 10% in 2015 to 20% in 2016. Healthcare leaders need to recognize the necessity and value of protecting patients' privacy to prevent thieves from altering peoples' medical records (Demshock, 2016; Votta, 2016). I arranged telephone interviews with healthcare leaders who combated identity theft and explored the strategies they use to reduce identity theft that led to medical identity fraud in other organizations.

Problem Statement

Medical identity fraud is a byproduct of identity theft that enabled imposters to obtain medical treatment, defraud patients, insurers, and government programs (Mancini, 2014) through forged prescriptions, falsified medical records, and misuse of victim's health insurance (Taitsman, Grimm, & Agrawal, 2013). In 2014, Federal officials lost $14.1 billion in improper payments to criminal activities (U.S. Government Accounting Office [GAO], 2016). The general business problem is that business performance in medical practices is diminished by identity theft and medical identity fraud. The specific business problem is that some healthcare leaders in medical practices lack strategies to reduce identity theft and medical identity fraud.

Purpose Statement

The purpose of this qualitative, multiple case study was to explore the strategies some medical practice healthcare leaders use to reduce identity theft and medical identity fraud to improve business performance. The population consisted of healthcare leaders at five medical practices in the state of New York who successfully addressed the identity

theft and medical identity fraud business problem. The implication for positive social change can result from improved healthcare services and reduced medical costs, leading to more affordable healthcare. Knowledge gained from this study could enlighten other healthcare leaders about innovative ways to protect the financial integrity of the healthcare system by identifying mitigation strategies to prevent future identity theft and medical identity fraud and thus increase business performance.

Nature of the Study

I chose the qualitative research method for this study to enable exploration of the effective strategies healthcare leaders use to reduce identity theft and medical identity fraud to improve business performance. Eide and Showalter (2012) stated that researchers use the qualitative method to better understand phenomena and gain insights from sampling a population and/or presenting statistical data to examine relationships between variables. Venkatesh, Brown, and Bala (2013) stated that researchers use the quantitative method when the goal was to gain insights from sampling a population or presenting statistical data to examine relationships or differences among variables. I did not choose the quantitative method because my goal was to capture participants' experiences rather than testing hypotheses for relationships between variables. I did not chose mixed methods because I did not seek to achieve a combined focus on statistical analysis and exploration of phenomena (Connelly, Sackett, & Waters, 2013; Venkatesh et al., 2013).

Within the qualitative method, there are several designs including phenomenology, ethnography, and case study. Scholars use the phenomenological design to understand participants' experiences better (Creely, 2016). Researchers use the

ethnographic design to develop new insights to understand peoples' beliefs, and cultural issues from a holistic viewpoint (Bhatti, Gørtz, & Pedersen, 2015; Reeves, Peller, Goldman, & Kitto, 2013). Researchers normally use case study design to explore people's lifestyles, managerial processes, the maturation of industries, and group behavior (Yin, 2012). Because I was interested in exploring the strategies used by a small number of medical practice healthcare leaders sharing similar positions but employed in different institutions, a multiple case study design was most appropriate for this investigation.

Research Question

What strategies do healthcare leaders use to reduce identity theft and medical identity fraud to improve business performance?

Interview Questions

1. What strategies did you use to reduce identity theft and medical identity fraud to improve business performance?
2. What hurdles did you face in developing and implementing strategies to improve business performance and how did you address the barriers?
3. How did you revise the strategies to address changing conditions?
4. What processes are in place to protect electronic records?
5. What processes are in place to protect paper records?
6. How did you stop an imposter from using other patients' identities?
7. What else would you add that we have not discussed regarding identity theft and medical identity fraud?

Conceptual Framework

The Health Insurance Portability and Accountability Act (HIPAA) was the conceptual framework grounding this study. In 1996, Congress enacted HIPAA to improve health coverage (Taitsman et al., 2013) and safeguard health records by limiting access only to authorized personnel (Mulig, Smith, & Stambaugh, 2015). The conversion from paper to electronic medical records made skeptics fearful that the privacy of patients' health records would be vulnerable to data breaches (Taitsman et al., 2013) by hackers and other intruders. Patients are assured of their privacy through healthcare organization's adherence to HIPAA standards, which is why HIPAA was the framework applied to this study. Through HIPAA, patients have clearly defined rights and access to their medical records (U.S. Department of Health and Human Services, 2016). I explored the findings from this study through the lens of HIPAA conceptual framework.

Operational Definitions

Cyberattack: Cyberattack occurs from the deliberate act to alter, change, deceive or destroy computer systems or networks to capture information or data for personal or financial use (Caplan, 2013).

Cybercrime: Cybercrime occurs from a criminal activity performed using electronic means to digitally steal data from computer systems or networks (Lagazio, Sherif, & Cushman, 2014).

Data breach: Data breach occurs when criminals gain unauthorized access to sensitive, proprietary or safeguarded data by compromising the confidentiality, integrity, and availability of information (Sen & Borle, 2015).

Fraud: Fraud involves the illegal practice to intentionally falsify facts misleading a person or groups promising goods or services for personal or financial gains (Policastro, & Payne, 2015).

Health information technology for economic and clinical health (HITECH): HITECH involves the procurement, access, usage, or disclosure of PHI that is assumed breached unless a covered entity or business associate demonstrates a low possibility of being comprised (Terry, 2014).

Unbundling: Unbundling involves a fraudulent act whereby clinicians or hospital officials submit separate invoices for patients' procedures billed as a single transaction per visits (Enthoven, 2014).

Upcoding: Upcoding involves a fraudulent act whereby clinicians use a higher payment rate to make patients' illness appears more serious to charge the most expensive costs for reimbursement (Jürges & Köberlein, 2015).

White-collar crime: White-collar crime (WCC) involves a practice that allows criminals to commit devious acts through deceit by disguising their illegitimate intent (Gaskin, 2012).

Assumptions, Limitations, and Delimitations

Assumptions

Brutus, Aguinis, and Wassmer (2013) defined assumptions as truth that cannot be verified. The initial assumption in this study was that participants would answer questions honestly, evade social pressure and personal biases during interviews. I also assumed that snowball sampling was possible, and healthcare leaders would refer me to

other subject-matter experts. A final assumption was that a multiple case study was the most appropriate design for exploring the stated business problem by preventing future identity theft and medical identity fraud and increase business performance.

Limitations

Limitations are factors that affect the outcome of a study (Brutus et al., 2013). The initial limitation involved telephonic interviews as they have potential weaknesses beyond the researcher's control that included the inability to view participants' nonverbal cues while answering questions. A related limitation was the inability to visit geographic locations in-person to conduct face-to-face interviews coupled with the small sample size, which may not have been sufficient to reach data saturation. Snowball sampling played a pivotal role in reaching saturation because it led to two additional participants.

Delimitations

Bartoska and Subrt (2012) stated that delimitations are boundaries researchers use as a restrictive tool. The first set of delimitations in this multiple case study focused on design, method, and location to explore the strategies healthcare leaders use to prevent identity theft and medical identity fraud to protect profitability. The second delimitation was the restricted target audience that led to a small sample size. The final delimitation was the decision to conduct telephone interviews instead of pursuing face-to-face forums and possibly increased the number of potential participants.

Significance of the Study

This study explored the strategies some healthcare leaders used to reduce identity theft and medical identity fraud to improve business performance. New York was

identified as one of three states recognized for fraudulent activities that led to medical identity fraud (Agrawal & Budetti, 2012) resulting in a compelling need to adopt new preventive and attenuation strategies to fight the medical identity fraud crisis. Identity theft led to falsified patient medical records, misdiagnosis based on inaccuracies in patients' records, followed by refusal and delays in treatment (Mancini, 2014). Agrawal and Budetti (2012) stated that identity theft resulted in higher co-pays, insurance costs, and denial of services in extreme cases and conditions.

Carlson, Lewis, and Nelson (2014) stated that financial losses from healthcare fraud in the medical system threatened the security and sustainability of hospital services. Exploring the strategies healthcare leaders' used to reduce identity theft and medical identity fraud provided solutions for healthcare leaders to improve business performance. Understanding strategies to prevent medical identity fraud would strengthen healthcare services for patients to get timely and suitable healthcare. Capturing the strategies of healthcare leaders' in small medical practices can offer insights to other leaders and possible solutions prevent or reduce identity theft and medical identity fraud and thus improve business performance.

Contribution to Business Practice

Findings from this study could help healthcare leaders improve business performance. Data breaches cost billions of dollars for consumers and leaders in organizations (Roberts, 2014); according to Romanosky (2016), cybercrimes cost $8.5 billion each year. Understanding the successful strategies some healthcare leaders use to reduce identity theft could help other leaders to preserve and strengthen their businesses'

performance by eradicating or reducing medical identity fraud on a global scale. Resolving the identity theft crisis is essential to eliminate thieves' devastation and thus increase business profits and performance by reducing fraud and sustain the healthcare industry. Results from this study may contribute to improved business practices by providing a mechanism to reduce identity theft and medical identity fraud, which can improve performance across the healthcare industry.

Implications for Social Change

Results from this study are expected to contribute to social change by increasing awareness and understanding of the successful strategies healthcare leaders use to prevent identity theft, which led to the medical identity fraud crisis. Reducing identity theft could prevent fraud for occurring by eliminating the high dependency for thieves to assume a person's identity before committing medical identity fraud under victim's name before impersonating their victims. The results of this study could play a pivotal role in protecting the financial integrity of healthcare systems by identifying mitigation strategies to prevent future identity theft and medical identity fraud crisis, which directly and negatively affects patients. Medical identity fraud places a major burden on patient care because of substantial revenue losses, but eradicating or reducing the crisis could affect positive social change by improved healthcare delivery, patient care, and attenuate the increasing cost of medical care for more members of society.

A Review of the Professional and Academic Literature

The objective of this qualitative multiple case study was to explore the effective strategies some healthcare leaders use to reduce identity theft and medical identity fraud

to improve performance in the healthcare industry. The identity theft business problem traveled beyond the borders of hospitals and medical facilities into peoples' residences. People, patients, and business professionals must protect social security numbers (SSN) and other sensitive data in their possession. One interesting point about identity theft is that thieves must acquire peoples' personal data before impersonating or using someone's personally identifiable information (PII; Tajpour, Ibrahim, & Zamani, 2013). After stealing someone's PII, imposters could intentionally commit medical identity fraud and acquired healthcare services under their victims' names without their knowledge. For example, breaches of PII led to 100 million names, addresses, passwords, and credit cards stolen because company officials refused to notify customers about the infractions (Anandarajan, D'Ovidio, & Jenkins, 2013). The objective of this section was to review current literature relating to the contributing factors that placed the burden on patient care due to revenue losses. Data from this professional and academic literature review provided solutions to improve business performance and strengthened healthcare services for patients to receive timely and suitable healthcare in the future.

Sources in this literature review came from multiple databases including (a) Business Source Complete, (b) ProQuest Central, (c) Sage, (d) Google Scholar, and (e) Emerald Management and utilization of available books. I gathered 158 sources peer-reviewed, dissertations, and scholarly articles--including (a) 10 books, (b) 148 peer-reviewed journal articles, and (c) 10 non-peer-reviewed articles. Of that total, 148 (94%) of the peer-reviewed articles were published within the past 5 years and 6% were published prior to 2011.

In the searches, I used the following terms included: *fraud*, *identity theft, medical identity theft, Medicare and Medicaid, physicians, clinicians, nurses and fraud convictions, victim identification, crime victims, criminal records, criminal law, property crimes, statutory law, criminal prosecution, personal information, thieves, cybercrime, identity fraud, insurance fraud, medical, healthcare fraud, fee-for-service, e-commerce theft, healthcare fraud, medical insurance, health,* and *fraud cases.* The search term *medical identity theft* revealed a total of 483 sources at Google Scholar while a search on *health care fraud* at Walden's Libraries returned 46,506 articles relating to *identity theft* and *fraud* in the healthcare system. Sources captured in this literature review were deemed relevant to the study of identity theft and medical identity fraud in the healthcare industry.

Health Insurance Portability and Accountability Act

The objective for conducting this study was to explore the effective strategies healthcare leaders used to reduce identity theft and medical identity fraud and improve performance. HIPAA was the conceptual framework grounding this study (Mulig et al., 2015). This conceptual framework was the central inductive process addressed the financial and personal embarrassment victims' experienced (Zivkovic, 2012) from healthcare fraud and abuse. Agris (2014) stated HIPAA focused on privacy and security rules limiting access only to authorized personnel to fulfill the intended purpose, disclosure, and specific request. HIPAA was critical to this study specifically because it was the official framework alerting patients of their privacy. Through HIPAA, patients

have clearly defined rights, and access to their medical records (U.S. Department of Health and Human Services, 2016).

Federal officials mandated Health Department representatives to comply with two primary regulations that centered on HIPAA and HITECH, according to Mohammed and Mariani (2014). Adoption of HIPAA led to confidentiality, integrity, and availability of sensitive data providing safeguards for PHI. Enabling separation of duties ensured healthcare providers, physicians, nurses, insurers, and other stakeholders afforded access only on a need-to-know basis to secure patients' privacy (Mohammed & Mariani, 2014). I explored the findings from this study through the lens of HIPAA, augmented by routine activity theory (RAT), the theory of rational addiction behavior (TORB) and rational choice theory.

Routine activity theory and theory of rational behavior. Routine activity theory (RAT) and Krstić's (2014) theory of rational addiction behavior (TORB) also served as conceptual frameworks for this study. RAT worked under the assumption that people intentionally made rational choices to commit crimes (Wang et al., 2015). Wang et al. used RAT to control crimes by targeting where to find and how to capture criminals, which served as a deterrent preventing thieves from committing crimes. RAT was not utilized to offer reasons why some people abstain from misconduct and what motivates others to commit crimes but it provided the means to explore situational and environmental factors of crimes (Wang et al., 2015).

When securing information that included PHI, RAT played an integral role when assessing the relationships between opportunity and vulnerability to correctly safeguard

patients' personal and sensitive records or data (Khey & Sainato, 2013). According to Khey and Sainato (2013), a noticeable increase in fraud led to $1 trillion losses in healthcare coverage attributed to national and international cybercrimes (Khey & Sainato, 2013) performed by criminals for personal and financial gain.

Wang et al. (2015) stated that the RAT concept operated under the assumption whereby people make rational choices due to motivation, opportunity, and when surroundings are suitable to commit violations. RAT was initially introduced to explain predatory criminal activities (Wang et al., 2015). The assertion of RAT claimed that certain people are capable of discouraging crimes and preventing them from occurring through the adoption of physical security (Wang et al., 2015). The theory involved four primary elements that included value, inertia, visibility, and access:

- Value involves the act of reducing risk relating to insider attacks by introducing internal resistance about improper use of functionality, movement of data and discovery to commit crimes. For example, criminals could steal information including names, phone numbers, SSNs, credit cards, bank accounts, and other consumer data trading such valuable information for sale on the black market.
- Inertia deals with the strength and control making it difficult for the internal perpetrator to steal information with malicious intent to control input, processing, and output to ensure accuracy and validity of criminal actions performed by an offender.
- Visibility occurs when a person realized the existence of a target knowing the whereabouts malicious actions.

- Access involved the action enabling offender or perpetrator to modify data due to necessity and needs (Wang et al., 2015).

Using TORB could lead to a better understanding of why some people make decisions for self-interests choosing the rationale only in the absence of excessive desires (Krstić, 2014). RAT and TORB frameworks were also suited in exploring the strategies some healthcare leaders used to prevent identity theft and medical identity fraud to improve performance. Both RAT and TORB theories provided insights regarding why some people make conscious decisions to commit crimes while others refrain from criminal misconduct, which could assist in prevention efforts.

Rational choice theory. Rational choice theory (RCT) was another theory also relevant for grounding this study. Becker (1968) introduced RCT economic approach of crime while Cornish and Clarke (1986) revisited the concept noting that some people purposefully make rational choices to commit crimes (Matthews, 2014). Cornish and Clarke asserted that people committed crimes by weighing the odds against the cost of not getting captured or punished (Matthews, 2014). The RCT concept was important to this study because imposters made rational choices and committed identity theft by impersonating victims and committed medical identity fraud for healthcare services after determining the risk was worth committing the crime. Understanding preventive strategies also include the understanding of deterrents making identity theft more difficult and less appealing for imposters who took calculated risk to impersonate people and commit medical identity fraud and received surgery under another person's name through falsification of patients' medical records (Taitsman et al., 2013).

Wortley and Mazerolle (2008) defined identity theft as a white-collar crime (WCC) and a rational choice (Madensen, 2009). Madensen (2009) stated that medical identity fraud fell under the purview of WCC relating to health care fraud. FBI officials defined WCC as a nonviolent crime for personal, financial, and organizational gain cited by (Champion, 2011). RCT provided the means to investigate medical practice leaders' decision-making strategies to deter potential impersonators and prevent identity theft and medical identity fraud crisis.

Healthcare Fraud Exposure

William Sherman, a former reporter at the *New York Daily News*, was the first person credited with uncovering and exposing health care fraud in 1973 (Reader, Jesilow, Pontell, & Geis, 1995). Sherman was the first person to uncover and expose healthcare fraud in New York City. Sherman posed as a Medicaid recipient and visited several Medicaid-connected providers in New York City, and other locales throughout New York Metropolitan area. While posing as a patient, Sherman realized physicians billed Medicaid for unnecessary services followed by overbilling for other medical services (Reader et al., 1995). Forty-four years later, fraud, waste, and abuse (FWA) continued to plague the Medicaid and Medicare systems and other government programs. A U.S. Government Accountability Office (2013) report indicated that costs totaled $555 billion for 49 million beneficiaries while improper payments cost $44 billion.

Mitigation Factors

For transparency measures, there was a paradigm shift in FWA laws that the federal government adopted due to an unlimited increase of healthcare fraud that placed

major emphasis on the refund recovery that started with the HITECH system. HITECH served as an extension for HIPAA as technology secured and safeguarded the protection of electronic records including patents' medical records, which showed applicability to this study. The problem could stem from easy access to PHI and PII that leads to illegal alteration, modification, and falsification to patients' records (Schweitzer, 2012).

PII involved peoples' sensitive data including driver's license number, credit card numbers, government identifications, electronic mail (e-mail) address, tax identification, passport number, and other pertinent consumer information (Tajpour et al., 2013). HITECH strengthened HIPAA by imposing stricter penalty totaling $1.5 million against criminals without exception to waivers and civil fines for a minimum of $50,000 (Mohammed & Mariani, 2014). Federal officials also recovered $4.8 million in fines imposed against New York Presbyterian Hospital and Columbia University for failure to safeguard patients electronic PHI (Kieke, 2014). Subsequent to HITECH, the Health Care Fraud Prevention and Enforcement Action Team (HEAT) also enforced government standards.

HEAT recovered $3.8 billion and returned $3.28 billion to the Medicaid and Medicare followed by recovery of $521 million during targeted federal audits (Jaeger, 2013). Dated back to 2007, HEAT Strike Force teams successfully convicted 1,800 criminals that stole over $7 billion from government programs (U.S. Department of Health & Human Service [DHHS] and Department of Justice [DOJ], 2016). HEAT officials led the largest healthcare fraud initiative involving $712 million as criminals' fraudulently billed insurance companies for payments (DHHS and DOJ, 2015). Joint

efforts between DHHS and the DOJ officials expanded the original fraud hot-spots for identity theft from three to nine major cities that included:

- Baton Rouge, Louisiana
- Brooklyn, New York
- Chicago, Illinois
- Dallas, Texas
- Detroit, Michigan
- Houston, Texas
- Los Angeles, California
- Miami-Dade, Florida
- Tampa Bay, Florida

Gaskin (2012) defined HCF as a WCC whereby criminals committed devious acts through deceit disguising their criminal intent (Gaskin, 2012). The interesting point about Gaskin's statement was that identity theft and medical identity fraud fell under the purview of WCC relating to HCF. FBI officials defined WCC as a non-violent crime for personal and financial gain harmful to company leaders' reputation (Champion, 2011; Gottschalk & Solli-Sather, 2011).

The magnitude and complexity of Medicaid and Medicare and unlimited funding made both programs lucrative targets for thieves to steal without fear of getting caught or punished. Physicians, nurses, other clinicians and medical identity fraud fraudsters continue to think of clever schemes resulting to FWA in the healthcare system. The federal government enacted HIPAA in 1996 to improve efficiency and effectiveness

requiring healthcare providers to provide safety and security of patients' privacy ensuring the protection of personal and other sensitive information (Burns & Peterson, 2010). Section 2, consisted of fraud schemes criminals used that included upcoding and unbundling, FWA; phishing, privacy data, identity theft, and medical identity fraud.

Advent of Electronic Activities

A distinctive feature of the human brain is the ability to form mental images of the future translating such vision to reality by combining computers and electronic images over the World Wide Web (WWW) or Internet (Leiner et al., 1997). Leiner et al. (1997) stated computers across the Internet revolutionized communications by uniting radio, telegraph, and telephone setting the stage for unprecedented integration of science and technology on a global platform. The WWW enhanced capability to rapidly disseminate information with precision from private and public entities within seconds anytime, anywhere in the world. The insurmountable Internet growth evolved to a collection of technologies satisfying the community needs starting with 394 million Internet users in 2000; 1.02 billion in 2005; 2.03 billion in 2010 escalating to 2.92 billion by 2014 (Statistic, 2015).

Commercialism of the Internet include private and commercial network services available by laptop, pager, and cellular phone led to a paradigm shift in competition for online businesses (Leiner et al.). Surfing the Internet moving from site-to-site conducting electronic-business, entering chatrooms, government sites, Facebook and electronic banks (electronic-banks) led to the phrase *cyberspace* (Hunter, 2003). Criminal activities involved credit card fraud; counterfeit drug and medicines; $100 million smuggling of

counterfeit handbags, wallets, purses, perfumes and identity theft coupled with 100 Panamanian children being victimized with counterfeit medicine consisted of diethylene found in illegal cough syrup followed by China, India, and Russian fraudsters that produced counterfeit medicines (Foltz, 2008; Przyswa, 2013). Cybercrime business problem needs more research as new thieves join forces with other criminals taking advantage of healthcare leaders (Cliff, 2015).

Fraud Theories

In-the-wild theory. The term "in-the-wild" is becoming popular again within the field of human-computer interaction (HCI). HCI was first introduced 29 years ago by Jean Lave (Crabtree et al., 2013). The in-the-wild concept focus more on creating and evaluating new technologies instead of observing existing practices making the theory differs from other approaches. Innovation and creativity spark growing interest regarding how persuasive new technologies (i.e., camera in Smartphone) are designed to enhance consumers' daily lives (Crabtree et al., 2013) but it led to a safe-haven for criminals in cyberspace. The arrival of an abundance of affordable "plug and play" technologies including cellular phone, ultrasonic, internet television and Bluetooth forever changed how people live today (Crabtree et al., 2013).

Fraud triangle theory. Fraud triangle theory in organizations was introduced by Steven Albrecht, founder of the American Association of Certified Fraud Examiners and President of the American Institute of Accounting (Yao, 2017). Triangle theory is based on three factors including opportunity, pressure, and rationalization. Figure 1 provides a graphical picture display of the three factors.

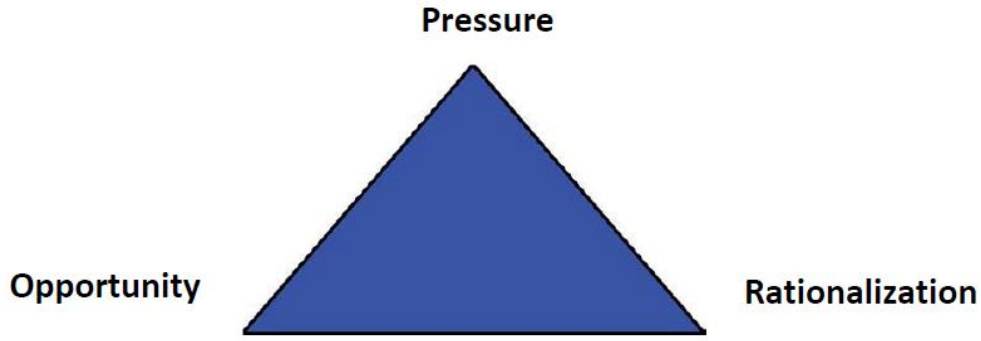

Figure 1. Fraud triangle theory.

Opportunity focused on the right condition and ability allowing a person or group to commit fraud. Opportunistic fraud is successful based on weak culture, controls, poor management oversight, and a leader's position or authority enabling thieves to conceal their illegal activity to prevent detection. Pressure deals with the incentive that drives and inspires a person or group to commit fraud (i.e., medical bills or prescription drugs to satisfy an addiction). For example, a manager with unlimited access to funds might commit fraud from the lack of oversight while employees may work collaboratively and commit fraud for personal and financial gain. Rationalization is predicated on thieves, fraudsters or imposters justifying their behavior and committing fraud. For example, criminals committing fraud by self-rationalizing and validating their actions claiming everyone is stealing it is no different if he or she commits fraud (Yao, 2017).

Fraud diamond theory. Fraud diamond theory (FDT) was introduced by Wolfe and Hermanson in the Certified Public Accountant Journal dated December 2004. FDT is an extended version of the Fraud Triangle Theory whereby it contained the same three factors including *opportunity*, *pressure*, and *rationalization*, followed by an additional factor titled: Capacity (see Figure 2). *Capacity* focuses organizational entitlement that

enables a person with the opportunity to commit fraud that is not normally granted to other people (Ruankaew, 2016; Yao, 2017). For example, a Chief Executive Officer with authoritative position and influence to perpetuate frauds based on his or her leadership position within the organization.

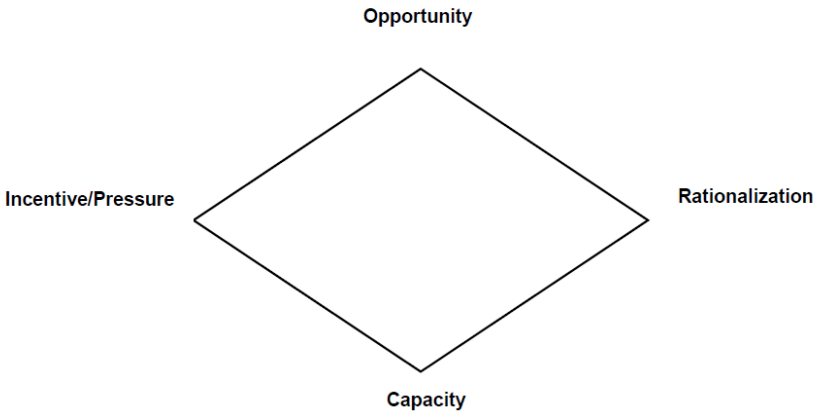

Figure 2. Fraud diamond theory.

Fraud pentagon theory. Fraud pentagon theory (FPT) is also an extension of the FPT was introduced by Crowe Howarth in 2011. The FPT theory contained five factors which include the same three factors of *opportunity*, *pressure* and *rationalization* followed by two new factors: *arrogance* and *competence* (see Figure 3). *Competence* deals with the ability for organizational employees to ignore internal measures stem from the capability to conceal social events for personal gain. *Arrogance* is the attitude of superiority leveraged from ownership rights believing organizational internal policies do not apply to he or she based on leadership position (Ruankaew, 2016; Yao, 2017).

Figure 3. Fraud pentagon theory.

Fraud GONE theory. The Fraud GONE theory focused on four factors to fraud including: Greed, Opportunity, Need, and Exposure (see Figure 4). *Greed* which is the desire to always acquire the most from situation includes stealing or committing fraud. *Opportunity* is dependent from the belief that the chance will present itself unexpectedly at any time. The opportunity's factor leads to a greater change to steal by members in top positions within an organization. *Need* drives and inspires fraudulent acts when a person's desire becomes urgent while *exposure* relates to capturing and penalizing perpetrators that committed fraud.

Figure 4: Fraud GONE theory.

Fraud MICE theory. The MICE theory is described as Money, Ideology, Coercion, and Ego (see Figure 5). Part of the theory expanded on the pressure side of the Fraud Triangle Theory resulting to motivating factors beyond non-shareable financial pressure. The Money and Ego factors are envisioned as the most common motivators for thieves committing fraud. Recent examples came from the demise of the Enron Corporation, Bernie Madoff Ponzi scheme and WorldCom leaderships were convicted for apparent illegal activities motivated by ego and money. Coercion defines the condition whereby a person is pressured into participating and committing fraud schemes. Ideology stemmed from committing white-collar crime through tax evasion by perpetrators claiming he or she paid enough taxes to the Internal Revenue Service. The fraud theories previously described above provides cleaver ways for thieves to adapt fraud schemes.

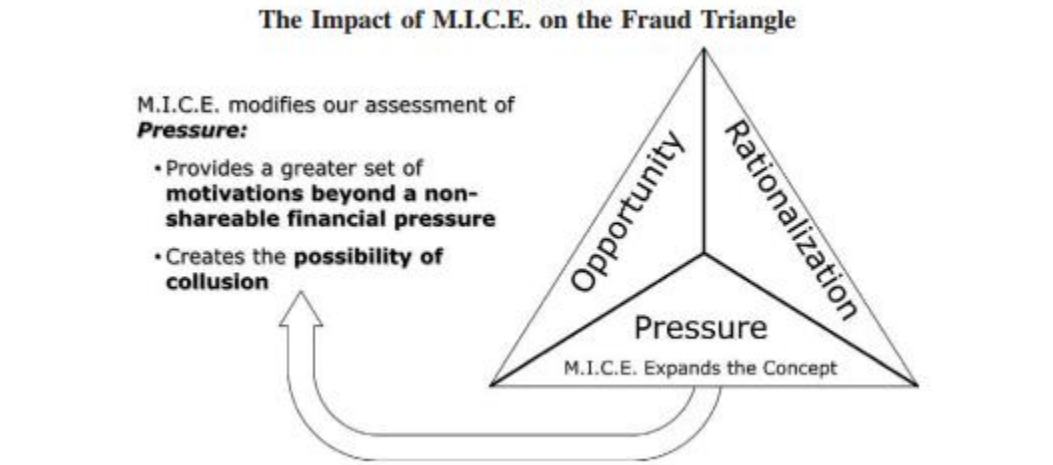

*Figure 5.*The impact of M.I.C. E. fraud triangle.

Fraud Schemes

Upcoding, unbundling, phantom billing and double billing. Upcoding occurs from the practice of separating procedure that is part of a total claim resulting to separate billing for each procedure (Januleviciute, Askildsen, Kaarboe, Siciliani, & Sutton, 2015). Upcoding is an economic factor that threatens survivability and sustainability of the healthcare industry. Government officials implemented the Prospective Payment System whereby hospitals received fixed payments from Medicare based on the diagnostic related group (DRG) limiting payments regardless of total costs patient expenses incurred (Januleviciute et al., 2015). To circumvent the DRG system, clinicians found innovative ways for patients to pay higher cost diagnoses by altering patients' care resulting to upcoding (Januleviciute et al., 2015).

Upcoding occurs between DRG pairs as providers submit a more expensive code for the most serious diagnosis even though the top-code was not present when the patient

was admitted or treated by a physician (Thornton, Brinkhuis, Amrit, & Aly, 2015; Vittadini, Berta, Martini, & Callea, 2012). For example, if a patient visited a physician and complained about having difficulty breathing and the doctor asked whether he or she felt symptoms of having a cardiac arrest. If the patient said no, the leading question could result in upcoding payment for a possible heart attack, even if it was later determined that the patient had a severe asthma attack that resulted in difficulty breathing. Another example, current procedures terminology code for a 1/2 hour visit to a physician is 99212 but when upcoding to 99213 or 99214 total costs led to $75,000 to $85,000 more profits per year respectively for a physician (Thornton et al., 2015). Upcoding is a fraud that must cease because it threatened survivability and sustainability of hospital operations, having a crippling effect on government programs that led to a negative impact on patients visiting hospitals for treatment to sustain their lives.

The second illegal practice, unbundling occurs when a provider charged for numerous codes appearing that the patients had several illnesses, but only a single condition existed (Thornton et al., 2015) leading to FWA. Unbundling involves separate claims including the ungrouping of healthcare services appearing as improper coding instead of being grouped into one claim (Enthoven, 2014). Phantom billing was the third illegal practice whereby providers filed false claims for health care services that were never delivered to patients (Thornton et al., 2015). Double billing is the final illegal practice as providers submit claims twice or multiple times attempting to acquire double payments for a single service provided to a patient (Thornton et al., 2015).

Fraud, waste, and abuse. U.S. government officials lose billions of dollars each year from imposters abusing federal programs and systems wasting precious resources by committing FWA. Thornton et al. (2015) claimed that FWA costs 2 trillion dollars in the United States with 33% of this attributed to frivolously spending. Criminals no longer commit crimes in broad daylight as healthcare WCC became the focus to steal funds. Moses and Jones (2011) noted that U.S. officials spent $808 billion in Medicaid and Medicare Services in 2010 and both scholars predicted that federal spending will cost $1.5 trillion by 2020. According to Gaskin (2012), WCC is a nonviolent action filled with deceit, deception, concealment, and breach of trust committed by healthcare providers, consumers, vendors of medical supplies or services, and healthcare entities.

Centers for Medicare and Medicaid Services (CMS) representatives predicted health care spending will increase to $4.4 trillion by 2018 and accounted for 20% of the U.S. gross domestic product (Moses & Jones, 2014). In 2009, government officials recuperated $1.63 in settlements based on healthcare fraud (Moses & Jones, 2014) but despite winning the judgments, WCC continued. Although U.S. officials keep adopting new programs including the PPACA of 2010, providing insurance protection for 30 million uninsured people and the upsurge in funds compounded FWA issues. For example, a physician assistant (PA) from California stole the identification of another PA, defrauding $7.7 million by prescribing durable medical equipment to recipients followed by three Floridian PAs who committed fraud totaling 130 million dollars (Moses & Jones, 2014).

FBI agent informational tips led to 839 indictments and 635 convictions due to healthcare fraud, restitution of $1.12 billion, 308 seizures totaling $61.2 million, followed by recuperation of $34 million from fines levied against criminals (Price & Norris, 2009). WCC continues to collapse the economy forcing the separation between poor, middle-class, and wealthy people depriving organizations and consumers needed resources to sustain lives. Detection and prosecution served as a tool to deter FWA, but the final goal calls for eradicating or preventing abuse from happening in the future. The point was that government officials adopted Medicare to provide health care for the elderly and Medicaid for low-income families with children and disabled person but unscrupulous thieves abused the system for personal and financial gains and it must cease before spiraling out of control.

Other cases of the economic costs of medical identity fraud in the United States alone led to $40 billion that affected 1.9 million victims (Mohan, 2014). For example, real-life experiences involved a crack-addicted pregnant woman from Oregon who impersonated another female's identity, stole her SSN, delivered a baby, and then abandoned the infant. Law enforcement later mistakenly arrested the actual victim and not the impersonator and placed the victim's children into foster care (Mohan, 2014). Following, a teenager was denied donating blood because an impersonator with HIV impersonated the teenager resulted in flagging the victim's SSN for having HIV (Mohan, 2014). The conclusion of FWA fraud schemes now leads to the False Claims Act.

False Claims Act (FCA). According to Stallings and Caravello (2013), the FCA was adopted during the Civil War period while Abraham Lincoln served as President of

the United States. The original FCA of 1863 levied sanctions on civilian personnel that submitted false claims to government officials and falsely acquired payment (Stallings & Caravello, 2013). From the inception of the 154-year-old act, several modifications occurred whereby people that intentionally filed false claims are subject to civil penalties. For example, false claims penalties increased from $2,000 per claim to a range of $5,000 to $10,000 (Stallings & Caravello, 2013).

Further FCA changes permitted private realtors (or whistleblowers) to file lawsuits against violators via *qui tam* actions in pursuit of FCA cases that played an integral role in prosecuting fraud on behalf of government entities (Stallings & Caravello, 2013). Penalties imposed under the FCA resulted in fines totaling $250,000 and 5 years imprisonment (Stallings & Caravello, 2013). A 1988 amendment to the FCA law was also adopted as government officials sought to remedy violations by reducing realtors' recovery to zero dollars for relators that initiated violations of the act.

Enactment of the 2010 PPACA and leverage from *qui tam* law enabled realtors to filed 6,199 FCA cases based on $13.6 billion in damages that resulted to the recovery of $2.2 billion in settlements and judgments (Stallings & Caravello, 2013). Further healthcare reforms sanctioned by federal officials' leveraged significant changes as DOJ and DHHS representatives' used *qui tam* provision to combat FCA cases (Patel & Sherer, 2016). In January 2016, a *qui tam* lawsuit was levied against David Bostwick, owner of Bostwick Laboratories, claiming Bostwick illegally filed false claims in the Medicare system for reimbursement of services not ordered by clinicians (Patel & Sherer., 2016). Bostwick improperly used incentives for physicians to steer patients to visit Bostwick's

Laboratories (Patel & Sherer, 2016). Federal officials determined that Bostwick violated the FCA, anti-kickback statute (AKS), and the physician self-referral law that resulted in a settlement between $2.6 and $3.75 million for receipt of full payment by the year 2021 (Patel & Sherer, 2016).

In 1972, federal officials enacted the anti-kickback statute (AKS), 42 U.S. Code § 1320a–7b that prohibited compensating for, accepting money for referring Medicare, Medicaid or other related federal government healthcare programs to protect against FWA (Patel & Sherer, 2016). AKS was defined as a criminal offense for any person to knowingly, and willfully petition, accept, offer or pay compensation to induce referrals or services for any healthcare-related program (Butler, 2016). In October 2015, Carl Reichel, the former President of Warner Chilcott's pharmaceutical company, violated the AKS law and repaid $125 million after pleading guilty for the criminal act (Patel & Shere, 2016). Based on allegations, Reichel coached company sales representatives who invited physicians that prescribed high usage of specific drugs and paid doctors approximately $600 to $1,200 and hired them as speakers at dinners hosted by Chilcott representatives.

Health care fraud became a legitimate concern as federal government officials consistently enacted various laws designed to prohibit illegal financial incentive leveraged by providers to entice physicians and other clinicians for healthcare services (Butler, 2016). For example, the initial Stark law was adopted initially in 1993 only to impose penalties for clinical services (Butler, 2016). Law-makers quickly expanded Stark's law to include sending or identifying data for a provider to charge for services not

rendered and acceptance of services in exchange for payment. Stark's law prohibited physicians from referring Medicare recipients to a designated health services entity whereby he or she has direct or indirect financial relationship including partial, full ownership or situation involving family members or friends (U.S. Government Accountability Office, 2016). Physicians who falsely filed claims to Medicaid or Medicare offices for payments of healthcare services in terms of prohibited referrals subject to violating certain provisions of FCA (U.S. Government Accountability Office, 2016).

Under the AKS, in Section 1128B(b) of the SSN Act, violators of the Stark's law are subject to fines totaling $25,000 and 5 years imprisonment imposed on criminals (Social Security Act § 1128B(b)). Butler (2016) alerted that ambiguity with Stark's law resulted in numerous labor hours spent by lawyers, consultants, and compliance subject matter experts to ensure compliance. PPACA officials recognized the need for healthcare reform and argued that fee-for-service program hampered the FWA laws. Congressional officials expanded the scope for the Secretary of DHHS to grant waivers for many FWA laws including Stark's law and the AKS statute. DHHS final waivers afforded extra protection from unnecessarily enforced Stark Law and other fraud for Medicare Shared Savings Program that outlined new and innovative approaches to healthcare delivery services (Butler, 2016; Dyer, 2015).

The examination of business literature revealed a series of purchasing fraud relating two cases in New York followed by a case in New Mexico. A Chief Executive Officer (CEO) at an International clinical partnership hospital for special surgery was

arrested for accepting kickbacks totaling $1.4 million (Mann, 2013). The CEO accepted $420,000 from hospital vendors and $298,500 from a hospital employee for negotiating and receiving funds from the employee's annual bonus followed by $670,000 from a British health care entity (Mann, 2013). The second indictment involved two employees from a Presbyterian Hospital in New York that was imprisoned for illegally awarded construction, maintenance, and service contracts totaling $2.3 million (Mann, 2013). In this case, 17 employees from six companies were convicted for accepting bribes. The final indictments involved Christus Saint Vincent Medical Center formerly known as Saint Vincent Hospital in Santa Fe, New Mexico (Mann, 2013). The Chief Operations Officer and Chief Financial Officer pleaded guilty to accepting $678,000 by approving payment totaling $3 million (Mann, 2013).

According to Butler (2016), Office of Inspector General (OIG) officials provided components relating to successful physician compliance and financial relationships including:

- Incentives from hospital officials violate AKS and similar federal or state laws;
- Joint ventures whereby business arrangements between physicians and hospitals officials resulted in services billed to federal programs including Medicaid or Medicare;
- Financial arrangement involving physicians services costs below fair market value; and,
- Self-referral law whereby physicians financial relationship violate Stark referral process posing major concerns for OIG representatives.

Attorney General Loretta Lunch joined forces with DHHS Secretary Sylvia Matthews Burrell and focused on a nationwide sweep led to 301 professionals including 61 doctors, nurses, and licensed professionals that resulted to $900 million in false claims (DOJ, 2016). Despite these laws and statutes, there are scores of documented criminal activities in the medical field including *phishing*, which is another fraud scheme interjected to cheat federal officials and consumers needed funds for health care services and other activities.

Phishing. Phishing occurs when fraudsters tricked people into sending personal data over the Internet to believe the request came from a legitimate source resulting to voluntarily release of sensitive information (Xu, 2012). Moore (2010) noted that the top two techniques used for stealing consumers' personal data were phishing attacks through entrapment and data breaches by infiltrating companies' computer networks resulting to identity theft. Moore stated that once people believe the request is real and responds by sending personal data, the information is redirected to a phony website for criminals to use the data and victimize innocent people. Data breaches were responsible for exposing millions of records stored in healthcare leaders' databases (Moore, 2010).

Spear-phishing is also another technique criminals' used by sending e-mails which seemed legitimate requesting specific data from people (Ferrillo & Singer, 2015). FBI agents alerted that criminals acquired employees' bank credentials by executing fraudulent wire transfers followed by phishing e-mails, keystroke loggers, remote access Trojans, and stole workers' credentials (Scanio & Ludwig, 2013). Illegal upcoding and

unbundling, FWA, phishing, and spear-phishing led to the exposure of private data exposure that potentially results in identity theft and medical identity fraud.

Privacy Data Exposure

HIPAA Privacy law was enacted to provide safeguard and protection for patients' health records limiting access to sensitive data only to authorized personnel (Mulig et al., 2015). The current push for digitizing patients' health records made federal officials fearful that privacy of health records could fall into the hands of cybercriminals during electronic exchange across the Internet (Mulig et al., 2015). Verbiage from a cyber-risk survey revealed healthcare leaders admitted they were unprepared for cyber-breaches due to the usage of smartphones, and similar devices that posed a security risk in the workplace (Bamrama, Singh, & Bhatt, 2013; Mulig et al., 2015). Despite concerns of security damages, 21% healthcare leaders did not update their computer networks while 12% refused to take corrective action believing data breaches will not affect their systems (Mulig et al., 2015). Exposure of privacy data was a major concern stemming from the inability to protect patients' PHI and safeguard of sensitive medical records led to fear, distrust, and privacy issues (Roberts, 2014) resulting to identity theft.

Data privacy continued to stay under scrutiny as computers enable linkage to digital information stored for easy access resulting to privacy risk to protect data (Li & Slee, 2014). Concerns for information privacy (CFIP) played a critical role in preventing personal and public digital data relating to improper disclosure in the digital world. Unauthorized exposure of patients' healthcare records either stolen or disclosed were extensively discussed from media alerts raising public awareness (Li & Slee, 2014).

Results from a study exposed 20,000 medical records containing names, SSNs, insurers, and diagnostic codes revealing patients' medical histories relating to mental health illness, cancer, and acquired immune deficiency syndrome (Li & Slee, 2014). Hospital officials in the United Kingdom also suffered intrusion and unauthorized disclosures of medical records involving thousands of employers and hundreds of physicians (Li & Slee, 2014). According to Li and Slee (2014), CFIP involved ways to identify and measure how critics perceived the collection of personal information and usage of personal data. CFIP consisted of four elements that included collection, errors, unauthorized secondary use, and improper uses:

- Collection–involve peoples' perception of the collection process regarding the acquisition of personal information for storage, distribution, and usage;
- Errors–focus on individuals' concerns about inadequate measures employees take to prevent deliberate or unintentional exposure to safeguard personal data;
- Unauthorized secondary use-involve the growing concerns regarding the collection, and usage of information other than its intended purpose both an; internal or external standpoint; and,
- Improper uses–dealt with individuals' concerns that unauthorized persons or thieves might illegally gain access to their personal information.

Cloud Technology

Cybercrimes gained new momentum becoming the most unreported crimes that made it lucrative monetarily for cybercriminals because of breaches escalated by 25% since 2014 (Rutkin & Tugander, 2015). As digitized data uploaded to companies'

networks, spies, intruders, and thieves conducted incessant cyber attacks to obstruct operations and steal data (Conkle, Wilson, & Sands, 2015). Regarding Cloud Services, Homeland Security officials responded to 256 incidents as 59% dealt with pipe and gas lines that stopped criminals from taking control of oil and gas systems (Huang & Du, 2015). Cybercriminals often gain access to healthcare leaders' network to inflict harm that was ideologically or financially motivated to punish victims by denying services while damaging healthcare leaders' reputation (Huang & Du, 2015).

Identity Theft

Identity theft was defined as the unauthorized use or misuse of personal information, or illegally using people's personal information for fraudulent activities including medical care, job, or government benefit (Harrell, 2015). DOJ officials claimed that 17.6 million people totaling 7% of U.S. residents (between the age of 16 plus years) became victims of identity theft while other findings revealed common types of misuse totaled 38% for banking accounts, and 42% for credit card accounts (Harrell, 2015). Anderson (2015) linked the economy crisis relating to fraud and identity theft due to high unemployment rates that possibly occurred from the U.S. recession. Anderson (2015) statement was not completely accurate as physicians, nurses, and other clinicians in the current workforce continued to commit fraud against federal and state programs credited for stealing $1.4 million per clinician (Pande & Mass, 2013). Identity theft became a major epidemic and crime of opportunity as thieves not only victimized people but they also committed medical identity fraud. Bamrama et al., (2013) alerted that thieves used

clever tactics such as spoofing and brute force attack against agencies' networks that led to major work stoppage from denial of services resulting to credit card fraud.

Statement from FTC officials centered around 8.3 million people that were victimized by identity theft dated back to 2005 and the continued to increase (Sharma & Baweja, 2017). For example, a 40-year-old patient was transported by ambulance to the cardiology clinic for rheumatic heart disease related issues. Echocardiography testing revealed immediate surgery was needed to save the patient's life and hospital inpatient experts obtained patient's consent and requested the patient's record. The original hospital denied the request because another patient received treatment for other health issues using the same name and SSN as the victim (Sharma & Baweja, 2017).

Monetary Effect of IT

The financial toll of PHI disclosure dated back to the 2005 exposure of 543 million records during 2,800 data breaches resulted to $13.3 billion in consumer financial losses (Romanosky, Hoffman, & Acquisti, 2014). Incessant unauthorized exposure of data breaches and identity theft placed enormous pressure on healthcare leaders to safeguard patients records (Romanosky et al., 2014) as intentional or unintentional negligence led to medical identity fraud. Most people blamed strangers for committing a higher volume of identity theft crimes but evidence proved that 70% of stolen personal data occurred between family members, co-workers, and friends (Tajpour et al., 2013) with access to PII at home and work that led to the root cause of medical identity fraud.

Before proceeding, it is important to understand the root-cause that leads to medical identity fraud. To achieve success, it was compulsory for criminals to steal and

acquire peoples' SSNs and procure personal identification before impersonating innocent people to commit medical identity fraud for surgery and healthcare services. According to Brody, Haynes, and Mejia, (2014), fraudsters scammed 5 billion in illegal refunds under other taxpayers' names that involved 51,700 cases followed by $21 billion in 2016. Part of the issue was the susceptibility of peoples' employee identification numbers (EIN) as employees' SSN and EIN appeared on federal W-2 forms, wage and tax statement. Dated back to July 2012, 1.5 million thieves fraudulently filed income tax returns and stole $5.2 billion in tax refunds (Brody et al., 2014). Despite government officials' implementation and enforcement of laws, statistics showed that identity theft became more prevalent in the United States and spreading across the globe (Hedayati, 2012). For example, 60% of all Americans and 25% of Germans shared passwords and accounts numbers with family, friends, and spouses resulting in 3% of Germans and 50% of Americans that experienced identity theft (Hedayati, 2012). The annual burden to fraud against United Kingdom citizens led to £1.3 billion or (1,718,080,000 U.S. dollars) followed by tax fraud of £215 million ($284,144,000 U.S. dollars), £400 million ($528,640,000 U.S. dollars) from money laundering and £584 million or ($771,814,400 U.S. dollars) for immigration and forging passports frauds (Hedayati, 2012).

Hospital Financial Pitfalls

Officials from the American Hospital Association conducted a survey and revealed that hospitals performance to determine their profitability measures included categories as either weak based on negative financial margins or strong due to positive operational margin (Bazzoli, Fareed, & Waters, 2014). Carlson et al. (2014) testified that

substantial losses and failure threatened the financial stability and sustainability of organizations. From a total of 2,971 hospitals, the study revealed that 24.6% medical facilities operated at financially weak levels, 13.4% performed at a mixture of weak and strong levels while 62% operated at financially strong levels resulting from the recession (Bazzoli et al., 2014). The first pitfall was that 47 hospitals closures occurred during 2010 to 2014 that left 1.7 million patients at great risk that stemmed from substandard healthcare due to abrupt stoppage of acute care and other healthcare services (Kaufman et al., 2016).

Medical travel to perform healthcare delivery services expanded globally to foreign soil including Panama Thailand, and India (Ruggeri et al., 2015) followed by 18 other countries. Physicians should not visit other countries to perform surgery until identity theft and medical identity fraud are under control. According to Ruggeri et al. (2015), precautionary measures must be taken to prevent harm, legal, and economic crisis in the healthcare system from the absence of regulation and lack of oversight. Based on increased fraud schemes, healthcare in the United States became out of control due to identity theft and medical identity fraud cheating nationwide residences from acquiring needed healthcare.

The expansion to countries with limited law enforcement will lead to uncontrollable fraud globally. The first threat regarding universal healthcare was systemic corruption resulting in adverse impacts for developed and resource-poor countries (Mackey & Liang, 2012). Foreign officials reported the scope of corruption led to billions of dollars annually resulting in 10% of global domestic product (Mackey &

Liang, 2012). The problem was that corruption and the mixture of fraud in healthcare lead to FWA followed by scarce resources impacted access to medical care, finance, and price inflation (Mackey & Liang, 2012).

According to Mackey and Liang (2012), corruption involved misuse of entrusted power for personal gain. For example, corruption in the United States alone led to fraudulent activities recovering $4 billion from enforcing officials, $163 million acquired from the indictment against organizational officials for overbilling leading to 5-10% medical expenditures (Mackey & Liang, 2012). On a global stage, the Cambodian government lost 5% of health budget due to corruption and fraud while Russian Federation officials lost 56% expenditures from fraudulent activities. Pfizer was fined $60 million for violating U.S. anti-bribery laws resulting from improper payments to healthcare clinicians in China, Russia, Bulgaria, Croatia, Kazakhstan, and Italy (Mackey & Liang, 2012). The influx of incessant fraud multilateral medical programs presents numerous opportunities for corruption in the healthcare systems. Developing countries do not have proper controls in place to protect finances, patients, and physicians' identities which could lead to identity theft and medical identity fraud because of bribery and other corruption (Mackey & Liang, 2012) in foreign countries.

Medical Identity Fraud

Medical identity theft became one of the fastest growing crimes that stemmed from identity theft (Taitsman et al., 2013). Medical identity fraud placed a tremendous burden on healthcare leaders and government programs deserving advance research on this growing topic (Taitsman et al., 2013). Conventional identity theft focused on

acquiring funds for personal and financial gain while medical identity fraud went beyond the financial burden affecting patients' and physicians' lives. From patients' perspectives, falsified medical records led to misdiagnosis and delay in treatments (Satter, 2014) that resulted to higher co-pays, insurance costs, and denial of hospital services (Agrawal & Budetti, 2012).

Federal officials adopted the HIPAA law based on security concerns followed by providing guidance to combat security threats (Kieke, 2014) but Hedström, Karlsson, and Kolkowska (2013) argued that employees' negligence and access resulted in exposure of name, date of birth, and other sensitive data found in patients' medical records. Medical identity fraud grew so lucrative that children became the newest target audience. Identity thieves' continue to steal 500,000 children's identities annually (Betz, Gudmunson, & Hong, 2012) requiring government officials, business leaders, and other stakeholders to collaborate; capture thieves and bring criminals to justice. Federal and State officials afforded health care coverage for 100 million participants via Medicaid and Medicare plus Children's Health Insurance Program (CHIP) resulting to one of four people in the United States (DHHS, 2014). Based on size and complexity of Medicaid and Medicare programs mentioned, theft became a lucrative target to commit fraud without fear of being caught as the Federal government continues to increase billions of funds in the system (DHHS, 2014) including enforcement actions to capture criminals.

For example, fraud schemes totaling $146 million enabled law-enforcement officials to capture 24 criminals in Texas followed by charges filed against 11 individuals in northern Texas for their involvement in a $47 million and $23.3 million scams.

Licenses physicians allowed unlicensed physicians to provide clinical services and send invoices for payment to the Medicare office (DOJ, 2016a). In California, healthcare fraud schemes tallying $162 million led to capturing 22 thieves followed by the incarceration of a physician for stealing $12 million. Following in Detroit, Michigan, 19 criminals were indicted for their involvement in fraud, kickback, and money laundering schemes that included distribution of drugs while false claims totaling $114 million based on unnecessary healthcare services followed by kickbacks of $36 million (DOJ, 2016b). Finally, in Tampa Bay Florida, 15 people were charged with various deceptions including pharmacy fraud and prescription drugs totaling $17 million and $8 million respectively for reimbursement claims (DOJ, 2016).

Criminals continue to focus on innovative schemes victimizing not only living people but also targeting deceased persons by procuring new identifications and drivers' licenses under deceased people's names with impersonators' photographic images (Daraiseh, Ahmad, Al-Joudi, Al-Gahtani, & Al-Qahtani, 2014). On a political and economic front, statistics revealed 10 million illegal immigrants from Mexico, South America, Asia, and Latin America living in the United States illegally stole peoples' identities and acquired SSNs, and driver's license to gain employment (Hedayati, 2012). Frequently visited social media networks including Facebook, Twitter, and Skype became a safe haven for hackers, imposters, and thieves to capture peoples' personal and sensitive data clearly posted in cyberspace. According to verbiage from a survey, 40% of consumers posted personal data online using weak passwords (i.e., citizens of France displayed their date of birth and passwords in clear view; Hedayati, 2012). The identity

theft economic crisis continuously spreading across the globe as thieves stole $2 billion annually from Canadian consumers, creditors, banks, and institutions followed by £1.3 billion in the United Kingdom (Hedayati, 2012). Identity theft became so rampant that thieves are targeting deceased people committing tombstone thefts.

Tombstone Theft

Tombstone resurrections occur when identity thieves stole deceased date of birth and names from newspaper obituaries and tombstones. Thieves' refused to permit deceased persons to rest in peace interjecting new innovative schemes by posing as insurance agents; contacting funeral homes, and acquired essential personal data on deceased persons (Hedayati, 2012). According to Hedayati (2012), war-driving was another clever tactic thieves used to acquire people's personal data illegally gaining access to consumers and institutions unsecured computer networks via wireless fidelity (Wi-Fi) or by using notebooks, and personal digital assistant (Hedayati, 2012).

Denial of Death Records

Social Security Administration (SSA) officials denied researchers access to the electronic availability of death records based on concerns about identity theft as a federal assessment of hospital security identified consumer fraud. SSA officials limit access to aid in preventing deceased identity frauds but scientific researchers, life insurance companies, banking and credit agencies, Internal Revenue Service (IRS) and the Centers for Medicare and Medicaid Services (CMS) personnel rely on the SSA death master file tracking system to keep track of deceased persons (Sack, 2012). Sack (2012) noted 7

million deceased names expunged from the SSA master file as the number grew to the point where IRS and CMS officials contemplated discontinuance the program.

Summary and Transition

This review of the professional and academic literature revealed a multitude of stories and fraud schemes within the healthcare system. During the past century, healthcare costs skyrocketed due to creativity and innovation in the medical field (Custer, 2016) coupled with incessant FWA. In terms of healthcare, identity theft played a critical role driving up costs to $5 billion for consumers and $48 billion for business leaders (Shackelford, 2012). Based on past and current literature, a wide spectrum of healthcare fraud and abuse existed in the medical field. Agrawal and Budetti (2012) reported the severity of medical identity fraud issues, for example, thieves stole 12,000 patient and physician identities for personal and financial gain. Impersonators adopted many schemes involving 49 phony storefronts using physicians' unique identifiers and committed fraud (Agrawal & Budetti, 2012).

Based on incessant fraud schemes, a compelling need exists for government officials, law-enforcement, clinicians, and other stakeholders to collaborate and find solutions to eradicate FWA in the healthcare system. Hackers committed 2,936 data breaches and 544,000,000 businesses related compromise dated back to 2012 (Holtfreter & Harrington, 2015). Other factors that require solutions to combat healthcare fraud include (a) insider jobs, (b) physical loss of records, and (c) unintended disclosure (Holtfreter & Harrington, 2015). Fraud placed a major burden on consumers and business

owners. The purpose of this qualitative multiple case study was to explore the strategies some medical practice HLs use to reduce IT and MIF to improve business performance.

In Section 1, I covered the following topics: the foundation of the study, background of the study, problem statement, purpose statement, and nature of the study, research questions and interview questions (see Appendix A), the conceptual framework, operational definitions, assumptions, limitations, delimitations a review of the professional and academic literature on fraud schemes.

In Section 2, I cover the following topics: the research plan, a restatement of the purpose statement, the role of the researcher, participants, research method, research design, population and sampling, ethical research, data collection instruments, data collection technique, data organization techniques, data analysis, reliability, and validity.

In Section 3, I began with an introduction, presentation of the findings, application of professional practice, and implications for social change. Other dialogs led to recommendations for action, recommendations for further research, and reflections.

Section 2: The Project

I used a qualitative multiple case study to explore the strategies some healthcare leaders use to reduce identity theft and medical identity fraud to improve business performance. In Section 2, I cover the following topics: restatement of the purpose, role of the researcher, participants, research method and design, population and sampling, ethical research, data collection instruments, data collection techniques, data organization techniques, data analysis, reliability and validity.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies some medical practice healthcare leaders used to reduce identity theft and medical identity fraud to improve business performance. The population consisted of healthcare leaders with leadership authority at five medical practices in the state of New York that successfully addressed the identity theft and medical identity fraud business problem. The implication for positive social change can result from improved healthcare services and reduced medical costs, leading to more affordable healthcare. Knowledge gained from this study would enlighten other healthcare leaders about innovative ways to protect the financial integrity of the healthcare system, and identify mitigation strategies to prevent future identity theft and medical identity fraud crisis to increase business performance.

Role of the Researcher

The role of the qualitative researcher involves the collection and analysis of data (Collins & Cooper, 2014). In performing the role, I served as the primary data collection instrument. I mitigated biases by avoiding personal inputs by abstaining from asking

leading questions and strived to view data collection from participants' perspectives. According to Scholl, Greifeneder, and Bless (2013), researchers should focus on establishing the truth by determining the direction to follow. For this study, I had no prior relationships with participants or with the research area.

In this study, I used the principles of the 1979 Belmont Report of the National Commission for Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont Report details the protection of participants in accordance with three principles: beneficence, respect for persons, and justice (Metcalf, 2016). Participants' confidentiality and their perspectives were respected (Fiske & Hauser, 2014). I mitigated possible personal bias by following a set of interview protocols with each participant, maintaining a researcher's log, and kept my thoughts and opinions separate from the data. In terms of rationale for interview protocol. I followed Brayda and Boyce (2014) and used open-ended questions and not deviate from the script by asking leading questions to get the desired results.

Participants

Eligibility criteria required that healthcare leaders be experienced reducing identity theft and medical identity fraud to improve business performance. I used purposeful sampling to select healthcare leaders at five small medical practices in the state of New York. Researchers progressively use purposeful sampling in qualitative research to identify and select information-rich studies relating to their phenomenon of interest (Palinkas et al., 2013). Purposeful sampling enable me to condense types and categories of strategies for gaining access to participants to provide recommendations for

multiple strategy designs (see Palinkas et al., 2013; Premalatha, 2016). Potential participants appeared on the websites of medical facilities and professional organizations; they received an invitational e-mail explaining the intent of the study. In addition to purposeful sampling, I also employed snowball sampling as a referral process or mechanism in which current participants are asked to recommend other subject matter experts for additional interviews to gain new insights from new perspectives (Bernard, 2013). The interjection of snowball sampling led to other suitable participants who wanted to share their insights on the identity theft crisis and subsequent medical identity fraud but were unavailable because of conflicting schedules.

Actions that developed effective working relationships with participants came from encouraging them to feel free to share their thoughts and perspectives, providing constant reminders stating they could cease from participating in the study without notice followed by listening attentively without interruption contributions. I emailed consent forms (see Appendix B) and requested written approval stating "I consent" before each interview that provided assurances of confidentiality. Regarding strategies for establishing a working relationship with participants, I began by asking each person to choose a date and time to conduct a 30-minute telephonic interview. Throughout the process, I encouraged questions and ensured participants were comfortable.

Research Method and Design

Research Method

The objective of this qualitative multiple case study was to explore the strategies some healthcare leaders used to reduce identity theft and medical identity fraud to

improve business performance. A qualitative method was more appropriate than a quantitative method for several reasons. Venkatesh et al. (2013) stated that researchers use the quantitative method to sample a population or present data in a statistical manner to examine relationships or differences between variables. Yilmaz (2013) noted that quantitative methods force researchers to use predetermined instruments to ensure it fits participants' perspectives. The quantitative approach would not focus on healthcare leaders' perspectives in determining the current strategies used to prevent medical identity fraud relying more on theoretical arguments (Goering & Streiner, 2013; Goertz & Mahoney, 2012), which was not conducive for the study. I did not choose the quantitative method because the objective of the study was to capture participants' experiences using strategies to reduce identity theft leading to medical identity fraud, instead of testing hypotheses for variables' relationships or differences.

The mixed method approach requires researchers to use quantitative and qualitative research to gain a universal understanding of a phenomenon of importance (Venkatesh et al., 2013). Leedy and Ormrod (2015) asserted that mixed research methods are reasonably complex requiring extensive researcher time based on the combination of qualitative and quantitative exploration. A mixed-method approach is a tool used to investigate prior studies and unexplored perspectives of participants (Serban & Roberts, 2016). I did not use a quantitative or mixed method because I do not intend to quantify data or present findings in a statistical form. Based on the qualitative research characteristics, I chose the qualitative research method for this study.

Research Design

I used the multiple case study design to explore the strategies medical practice healthcare leaders used to reduce identity theft and medical identity fraud to improve business performance. Other research designs were considered, that included ethnography, grounded theory, and phenomenology. Researchers use the ethnographic design to develop new insights to understand beliefs, and cultural issues from a holistic viewpoint (Bhatti et al., 2015; Reeves et al., 2013). Scholars use grounded theory when there is a need to develop theories stemming from the collection of data to explain human interaction (Lawrence & Tar, 2013). Johnson (2014) viewed grounded theory as a qualitative research design tool to develop theories of a process or action predicated on perspectives from a large group of participants. One scholar argued that researchers use the ground theory design to suppress ideas, and practices abstaining from openness to current perspectives to maintain their importance (Campbell & Stanley, 2010; Lo, 2014).

According to Premalatha (2016), grounded theory qualitative research designs are used to transpire theories from rich data acquired from various stakeholders. Based on the views above, I did not use grounded theory because the intent of this study was not to develop theories. The final design considered but not selected was phenomenology. Moustakas (1994) claimed that scholars use phenomenological research to understand human experiences, behavior, and relationships as others believe that phenomenological focus on interpreting the human factors of peoples' life experiences and how each person views their surrounding (Applebaum, 2012; Wells, 2013). Creely (2016) claimed that phenomenological research is used to better understand participants' experiences

requiring researchers to set-aside personal biases, attitudes, and beliefs refraining from judging people.

Because I am interested in the perceptions of individuals within a bound place and time, multiple case study was most appropriate. Rubin and Rubin (2012) claimed that two to three interviews were adequate to achieve ample sample size to solicit responses from participants. Denzin and Lincoln (2013) asserted the possibility of achieving data saturation with 10 participants. Following Rubin and Rubin's (2012) guidance, I was able to achieve data saturation by interviewing 5 participants, one participant at each of the five medical practices in the state of New York. I continued interviewing participants until data became repetitive, which leads to data saturation. Data saturation occurs when a considerable amount of information is collected and extra data cease to provide new insights into a study (Baškarada & Koronios, 2014; Wittmayer, & Schäpke, 2014).

Population and Sampling

When justifying the sampling method, researchers progressively use purposeful sampling in qualitative research to identify and select information-rich studies relating to the phenomenon of interest (Palinkas et al., 2013). Loh (2012) used purposeful sampling to interview doctors transitioning from clinical practice to senior hospital management. Loh's interviews led to the collection of qualitative data based on doctors' belief, knowledge, and opinions. Loh's purposeful sampling technique sets the precedent to explore the strategies healthcare leaders used to reduce identity theft and medical identity fraud to improve business performance, which was critical to this study.

After IRB approval, the research for potential participants lasted for 30 days. During that period, I started with Google, Dogpile, and other search engines via the internet and found several numbers to medical practices resulting to eight recruits. Of the eight potential participants, two participated in the study. I visited small medical practices where seven expressed interest but only one respondent participated in the study. Snowball sampling led to five additional recruits of which only two participated.

I conducted interviews with five participants from five small medical practices. Rubin and Rubin (2012) claimed that two to three interviews were adequate to achieve ample sample size to solicit responses from small groups of participants. On the opposite end of the continuum, Ball (2010) argued that researchers reached saturation only after interviewing at least 26 participants. Based on Rubin and Rubin's assertion that two to three interviews were adequate to achieve ample sample size to reach saturation, I chose to interview five healthcare leaders. Saturation point which occurred after interviewing the fourth participant during the study.

A smaller sample size helps to achieve saturation faster (Fusch & Ness, 2015). Failure to achieve data saturation negatively impacts the validity of the study (Fusch & Ness, 2015). Francis et al. (2010) argued that researchers reach data saturation sooner from participants with similar experiences using purposeful samples. I ensured data saturation by carefully following the determined interview protocol with participants who met strict requirements for participation, including those with similar experience of successfully implementing strategies to reduce identity theft and medical identity fraud.

Criteria for selecting participants specifically included healthcare leaders who experienced implementing strategies to reduce identity theft and medical identity fraud in order to improve business performance. All participants participated in telephonic, semistructured interviews. This approach allowed the research setting to be that of the participant's choice. Researchers conducting telephone interviews help participants to feel comfortable as people use telephone daily to communicate with friends and family (Straus, Johnson, Marquez, & Feldman, 2013; Ward, Gott, & Hoare, 2015). Although Farooq (2015) opposed telephone interviews, stating face-to-face settings yield superior data collection, a telephonic interview was appropriate to allow for flexible scheduling.

Ethical Research

I did not collect any data or conduct interviews with potential participants without IRB approval. After IRB approval (Walden IRB No. 10-11-17-0533495), I contacted potential participants and discussed the process before scheduling interview appointments. Afterwards, I send a consent form to participants via e-mail. The consent form (see Appendix B) provided a complete description along with an explanation of the study. Participants with desired interest returned the consent form indicating their consent by replying with the words "I Consent" via e-mail and retained a copy of the consent form for their records.

According to Bristol and Hicks (2014), there are inherent ethical risks involved with recording participants' perspectives as it could jeopardize interviewees' privacy, trust, and confidentiality. Proper selection of willing participants leads to satisfactory results ensuring the validity of research projects (Bristol & Hicks, 2014; Miller et al.,

2013). Participant procedures for withdrawing from the study was that they reserved the right to withdraw prior to, during, or after providing their perspectives for the study. Each participant had the option to send an e-mail at any point stating their intent to withdraw from the study. Additionally, I informed participants that the study was strictly voluntary with no incentives for participation. I mentioned to each participant that representatives at Walden University will respect their decision to participate or not take part in the study as indicated in the consent form.

I took several measures by averting from conducting danger experiments opting to telephonic interviews preventing harm to participants that assured the ethical protection of participants. According to Cugini (2015), it is paramount to the rights of participants to prevent harm or danger to their safety. I did not collect data before receiving Institutional Review Board (IRB) permission from Walden University. I used the 1979 Belmont Report written by the National Commission as a guide to protect human rights during this study. The Belmont report worked under three principles (a) beneficence, which deals with the principle not to harm participants; (b) respect for persons, people have the right to participate or not partake in a study; and (c) justice as researchers are expected share results of the findings whether it is good or bad (Sims, 2010).

Upon completion of this study, full protection of interviewees' voice recordings and other data safeguarded will remain in a fireproof safe at my residence in New York for 5 years. After 5 years, I will destroy all voice recordings. Participants' identities, names, and organizations will remain confidential at all times. I referred to participants

involved in the study as Participant 1 or (P1), Participant 2 (P2) and Participant 3 (P3) consecutively until conducting the final interview.

Data Collection Instruments

For this qualitative multiple case study, I was the primary data collection instrument. According to Birley and Moreland (2014), researchers use interviews, surveys, testing, and questionnaires as instruments for collecting data for research. I used telephonic semistructured interviews and explored the strategies healthcare leaders used in the state of New York to reduce identity theft and medical identity fraud and improved business performance. According to Baškarada and Koronios, (2014), stated that researchers use interviews as a collection instrument to capture experiences and perceptions.

Miner-Romanoff (2012) stated that an interview protocol aids immeasurably in conducting studies. When it came to process and protocol (see Appendix C), I began the interviewing process by greeting each participant starting with a good morning or good afternoon. I provided my name and made participants felt comfortable by asking, how are you doing today? Prior to meeting with participants, I received the consent form via email, ensuring they had time to read, understood the process, and signed the consent form (see Appendix B) replying via e-mail with “I Consent”. I alerted participants prior to turning on the recorder to allow ample time for them to agree or disagree. All participants were asked the same interview questions. Before ending each session, I thanked each participant for participating in the study and sharing their perspective during interviews.

To enhance reliability and validity, I utilized member checking for participants to review the perspectives captured during one-on-one telephonic interviews. Member checking provided each participant the opportunity to decide whether my interpretation of the data captured was accurate. The member checking process occurred via e-mail, with a follow-up phone call to ensure clear communication with participants.

Data Collection Techniques

I used Google, Dogpile, and other search engines via the Internet and located phone numbers to small medical practices in the State of New York. I contacted 20 potential participants and initially 15 expressed interests to take part in the study. I did not collect any documentation but instead acquired phone numbers and e-mail addresses from a total of 20 interested participants. I gained access by visiting and calling participants followed by the snowball technique that led to two participants. Interviews were not conducted until IRB approval was received. After obtaining IRB approval, I visited five small medical practices in the state of New York and explained to HR personnel that I was conducting research to fulfill the requirement for a doctoral project. I requested and met with healthcare leaders and a total of 15 of 20 expressed interests to participate which later shrunk to 10 participants.

In the end, five of 10 participated because the remaining five had conflicting schedules that prevented them from participating in the study. I conducted semistructured telephonic interviews with five participants who answered seven open-ended questions that lasted between 10 to 33 minutes on the telephone. A few extraordinary things that happened started with two participants that shared their experiences with identity theft

that led to medical identity fraud. The other extraordinary occurrence came from acknowledgement from participants 3 and 5 stating they adhered to HIPAA which providing confirmation to the conceptual framework for this study.

I followed-up with interested individuals via e-mail, send a copy of the Consent Form (see Appendix B) to each participant and gained their approval to participate in the study. The consent form started by inviting participants to part take in the study, background information, procedures, voluntary nature of the study , risk and benefits of being in the study, payment, privacy, contact and questions and acquiring the statement of consent. I provided a full interview protocol (see Appendix C) followed by an abridged interview protocol that included 11 step to follow during interviews. I first received permission to record each interview.

I used a Sony ICD-PX440–Digital Voice Recorder with a built-in 4-gigabyte flash memory that had a file transfer capability to a personal computer. I also had a Samsung Galaxy S7 cellular phone for backup recording in the event the Sony ICD-PX440 primary device became inoperable or malfunctioned. The Sony ICD-PX440 recorder did not malfunctioned eliminating the need to use the Samsung Galaxy 7 backup device. After receiving participants' permission to record, I started each session by conducting the following actions:

- Greeted each participant and asked if he or she had any questions;
- Reiterated the title of the topic and intent for conducting the interview;
- Ensured each person retained a copy of the consent form;
- Alerted participants that the recording device would be turned on;

- Upon receipt of participants' favorable approval, I turned on the recording device;
- Asked for clarification if their perspective was not fully understood;
- I reminded participants that in 2 weeks; they will be asked to confirm my interpretation of their perspectives via member checking; and,
- After interview sessions, I thanked each participant for their contribution.

Johnson et al. stated that qualitative collection techniques consist of telephone interviews, document review, visiting facilities to conduct face-to-face interviews, data recording, and visual media. Based on time constraints to complete the study, I conducted telephonic interviews and data recording that captured the perspectives of participants. Based on time constraints to complete the study, I conducted telephonic interviews and document review by utilizing literature review documentation followed by data recording from perspectives shared by participants. The advantage of semistructured telephonic interviews claimed that participants felt comfortable as people use telephones daily to communicate with friends and family as interviews can take place in a location of their choosing (Straus et al., 2013; Ward et al., 2015). Disadvantages when conducting telephone interviews include the inability to see facial expressions and body language. Guo et al. (2012) noted that during face-to-face interviews positive or negative indicators, including eye contact, attitude, facial expressions, and head movements help to recognize sincerity or insincerity.

Member checking results to a quality control mechanism that researchers use to enhance trustworthiness to gain respondent validation (Birt, Scott, Cavers, Campbell, &

Walter, 2016). Researchers use member checking as an instrument to validate, verify, and assess the trust between researcher and participants providing interview transcripts for respondents to check, pinpoint errors, and verify correct interpretation of data (Birt et al., 2016). For this study, I ensured that all participants afforded the opportunity to conduct member checking and ask respondents to return responses to me within 3 days via e-mail. I also notified participants that a non-response after 3 days was considered acceptance of my interpretation.

Data Organization Techniques

The collection of data for this qualitative multiple case study came from document review and participants' responses shared via open-ended questions during telephonic interviews. I created an Excel Spreadsheet and filed participants' interviews under separate names according to the interview dates and stored each file in a designation folder located on my computer's hard drive. I also maintained a backup copy of each file on a universal serial bus (USB) flash drive or what is commonly known as a USB thumb drive in case of file corruption. For example, if interview 1 was conducted on 10 June 2017, it was coded as *P1.06.10.2017*. I also color-coded each participant interview to organize and identify files (i.e., P1 was coded *blue* followed by a *red* for P2) and other colors for subsequent participants.

According to Chittem (2014), computer-assisted software is an enhancement tool researchers should use to analyze data for qualitative analysis. I imported the Excel Spreadsheet into NVivo 11 Pro for Windows software by manually typing the information which aided in analyzing each participant's perspectives shared during one-

on-one telephonic interviews. I am retaining all information collected during this study for a period of 5 years and maintain in a fireproof safe located at my residence in the state of New York. After 5 years, I will permanently destroy all recorded data to protect participants' privacy.

Data Analysis

The appropriate data analysis process for this qualitative multiple case study was methodological triangulation. Taylor, Bogdan, and DeVault (2015) stated triangulation occurs from using various techniques and different means to acquire participants' perspectives. The resources for collecting information came from literature review documentation and semistructured telephonic interviews. Literature review documentation provided added insight into the strategies some healthcare leaders used to reduce identity theft and medical identity fraud that might not be able to share within the framework of semistructured interviews. After completion of data collection, I organized and analyzed participants' responses captured during telephonic interviews.

Yin (2014) stated that researchers use data analysis as a tool to organize, assess, extract, and interpret information collected from participants. The logical and sequential process for the data analysis consisted of Yin's five-step process by assembling or acquiring data, disassembling by organizing data to find commonality or themes, re-accumulating by matching data established from common themes, interpreting and reaching a conclusion by analyzing the data shared by participants. I used the Excel spreadsheet and assembled perspectives participants' shared during telephonic interviews and compiled the data in a logical sequence. I imported the data into the NVivo software

which is a useful tool researchers' use for analyzing qualitative data according to (Edward-Jones, 2014).

Additionally, I used NVivo to organize the data and disassemble participants' input by searching for key themes before moving to the next stage of reassembling data collected from identified themes. Following, I interpreted the data and provided a conclusion from participants' interviews, and literature review. The utilization of Excel spreadsheet and NVivo are useful tools for qualitative data analysis. For example, if a study has five or less interview questions, I suggest using an Excel spreadsheet because the process could be less labor intensive. Subsequently, if a study involves six or more interview questions, I encourage researchers to use the NVivo software because it is an effective tool to identify codes, and themes for fast visualization and swift analyzation. Results from the NVivo software could lead to success because it enables expediting, organizing and analyzing data.

I focused on key themes that emerged by searching for congruencies between participants and within document review. Following Yin's five-step process of assembling, disassembling, re-accumulating and conclusion, I used an Excel spreadsheet along with NVivo and organized the data that enabled me to focus on key themes. Doing so, I was able to correlate the findings with my conceptual framework and sources within my literature review which led to the conclusion.

Reliability and Validity

Reliability

Reliability became the tipping point whereby findings and outcomes are replicated by researchers or investigators to ensure accuracy by reading, re-reading and listening to recorded interviews (Pozzebon, Rodriguez, & Petrini, 2014). Dependability centers on producing comparable or similar findings if the process occurs as defined (Barry, Chaney, Piazza-Gardner, & Chavarria, 2014; Pozzebon et al., 2014). For this multiple case study, I addressed dependability by using member checking of data interpretation that allowed participants an opportunity to review the data captured. Member checking helped to ensure accurate representation of participants' perspectives, experiences, and enhance transparency.

Validity

Validity. Transparency was important as Yin (2014) suggested because it leads to credibility, readability, and confirmability of data that could be misrepresented or not statistically measurable. In addition to using member checking to address dependability, member checking also helped to ensure credibility. I used member checking to ensure credibility along with methodological triangulation by collecting data from both literature review documentation and from semistructured interviews.

Transferability. Transferability leads to the ability to relocate results or findings to others (Pozzebon et al., 2014). Frels and Onwuegbuzie (2013) believed that there is a compelling need to educate business leaders, consumers, and victims of identity theft leading to medical identity fraud. Although transferability is ultimately the reader's

responsibility (Elo et al., 2014), I provided rich descriptions and thorough details to help make transferability possible.

Confirmability. Confirmability enabled researchers to capture evidence to corroborate their findings resulting in the accurate and credible interpretation of data (Pozzebon et al., 2014). Van Biljon (2014) noted that interjecting biases in the interpretation of data should be avoided. To abate biases, I carefully followed my interview protocol and employed triangulation.

Data saturation. Data saturation normally occurs when new information or evidence cease, resulting in repetitive data from participants (Fusch & Ness, 2015). One of the unknowns for this study was the actual data saturation point. I continued to interview participants until reaching data saturation whereby respondents' answers became repetitive and no new information was provided from additional interviews.

Summary and Transition

The purpose of this qualitative multiple case study was to explore the strategies some medical practice healthcare leaders used to reduce identity theft and medical identity fraud to improve business performance. Prior to IRB approval, I did not collect any information or conducted interviews with potential participants without IRB approval. After IRB approval, I began the data collection process for this study that included semi-structured telephone interviews with five participants in the state of New York. During interviews, I used seven open-ended questions to gather their perspectives. In visiting small medical practices, seven potential recruits expressed interest but only

one respondent participated in the study. I also used the snowball sampling technique that resulted in five additional potential recruits and two participated.

I utilized member checking that enabled participants to review the perspectives captured during one-on-one telephonic interviews enhancing reliability and validity. Member checking provided each participant the opportunity to decide whether the interpretation of the data captured during interviews were accurate. I created an Excel spreadsheet and filed participants' interviews under separate names and stored each file in a designation folder on my computer's hard drive. Upon completion of transcript, I imported the Excel spreadsheet in NVivo 11 Pro for Windows software which coded the data in themes.

In Section 2, I presented the methodology of this multiple case study, including data collection, organization, and analysis. I also provided data related to reliability, dependability, and validity focusing on credibility, transferability, confirmability, and data saturation. Section 3 of this qualitative multiple case study shifted to presentation of findings, application to professional practice, implications for social change, recommendations for action, recommendations for future research, reflection, and conclusions.

Section 3: Application to Professional Practice and Implications for Change

The objective of this qualitative multiple case study was to explore the strategies some healthcare leaders used to reduce identity and medical identity fraud to improve business performance. I describe the different ways that the findings about participants' perspectives confirm, disconfirm, and extend knowledge in comparison to peer-reviewed studies. In Section 3, I present the findings, applications to professional practice, implications for social change, recommendations for action, further research along with reflections and conclusions.

Introduction

The purpose of this qualitative, multiple case study was to explore the strategies some healthcare leaders used to reduce identity theft and medical identity fraud to improve business performance. Telephone interviews with five small medical practice healthcare leaders in the state of New York generated a plethora of information for this study. Following interviews, I examined the perspectives shared by participants from small medical practices and gained new insights from their strategies to combat against identity theft that led to medical identity fraud. Analysis of materials collected from participants resulted in the identification of 56 codes and five major themes.

Based on the analysis of the information, the five themes emerged: (a) training and education, (b) technology, (c) protective measures, (d) safeguarding PII data, and (e) insurance. Of the 12 sub-themes, one, titled HIPAA, emerged from the main theme *protective measures*, and added validity as P3 and P5 used HIPAA, the primary conceptual framework that grounded this study (Taitsman et al., 2013). Data captured

from interviews revealed the successful strategies some healthcare leaders' use to increase business performance. Following interviews, I transcribed and examined the perspectives shared by participants, which resulted in 56 codes and five major themes.

Presentation of the Findings

Results from this qualitative, multiple-case study addressed the overarching research question: What strategies do healthcare leaders use to reduce identity theft and medical identity fraud to improve business performance? I conducted five telephone interviews with healthcare leaders, which lasted from 10 to 33 minutes and yielded an abundance of data. In the interviews, I used seven open-ended questions and subsequently distributed the transcripts for member-checking (all of which were approved). As suggested by Elo et al. (2014), qualities of qualitative analysis findings from open-ended questions are critical for validity and reliability of the data collected.

The numbering scheme used for participants started with Participant 1 = P1, Participant 2 = P2, and continued with the same pattern until the final interview ended with P5. From the inception, 15 potential participants expressed interest to part take in the study. The end result, only five participated in the study due to conflicting schedules that did not permit time for interviews. Utilization of methodological triangulation played a pivotal role in soliciting willing participants as per (Yin, 2013). Saturation point started with the second interview and ended after the fourth participant but I interviewed the fifth participant because it was the participation goal of five healthcare leaders for this study. Each participant understood their involvement was voluntary as provided on the consent form sent via e-mail. Participants agreed via e-mail replying with the words "I consent"

and shortly thereafter voluntarily participated in the study based on scheduled appointments.

Upon completion of the responses, and updating the Excel Spreadsheet used to capture participants' perspectives acquired from telephonic interviews, I uploaded the spreadsheet into NVivo 11 Pro for Windows resulting to visualizing data through graphs, cluster analyses, models, and reports as recommended by Edwards-Jones (2014). The five themes developed from the utilization of NVivo aligned with the conceptual frameworks grounding this study including HIPPA, routine activity theory, the theory of rational behavior, and rational choice theory. Five major themes relevant to this study were: (a) training and education, (b) technology, (c) protective measures, (d) insurance, and (e) safeguarding PII data. Table 1 shows frequency of codes that led to five major themes.

Table 1

Frequency of Major Themes

Major theme	*N*	Participant
Training and education	11	1, 2, 3, and 5
Technology	13	1, 2, 3 and 5
Protective measures	42	1, 2, 3, 4, and 5
Safeguarding PII data	11	1, 2, 3, 4, and 5
Insurance	15	1, 3, 4 and 5

Note. *n* = frequency.

In reviewing Table 1, the frequency of the first major theme *Training and Education* totaled 11 participants consisted of P1, P2, P3, and P5. For Theme 2, the frequency of *Technology* totaled 13 participants including P1, P2, P3, and P5. Following with theme 3, *Protective measures* frequency usage totaled 42 times by participants P1, P2, P3, P4, and P5 while Safeguarding PII data frequency totaled 11 including P1, P2,

P3, P4 and P5 with *Insurance* frequency totaled 15. For a better understanding of major theme and sub-themes, let start the examination process with Training and Education.

Theme 1: Training and Education

Training and education was the first major theme that emerged from exploring the strategies that some healthcare leaders used to reduce identity theft and medical identity fraud to improve business performance. Based on participants' responses regarding training and education the following subthemes emerged including (a) train employees, (b) train patients, and (c) educate consumers. Table 2 below illustrates the frequency of codes used by participants followed by which participant provided the responses.

Table 2

Subtheme Developed from Training and Education

Subtheme	*N*	Participant
Train employees	5	1, 2, 3, and 5
Train patients	3	1, 3, and 5
Educate consumers	2	3 and 5

Note. *n* = frequency.

Participant 1 noted,

> I often ask my staff, if that was your personal data would you want it protected? We use a variety of things such as rounding out with the frontline workers and the senior team. We use as part of our quality check, joint commission, and accreditation, and watch to see if clerks use the two-person identifier. If not, we'll reinforce with training. We are transitioning to the Kiosk system and still in the process of doing that. The idea was to check-in every patient through the Kiosk

> system that has some built-in internal controls to help validate and verify the individual's information.

Participant 2 stated

> The first thing that we do starts with training our staff on Privacy Act and information awareness. Training involved care and safeguarding of personally identifiable information such as social security numbers, home-addresses, patients' disability and the nature of their disability, ensuring pertinent data properly safeguarded. Information is only shared on a need-to-know basis!

Participant 3 went beyond by training employees stating that "patients are encouraged to request a review of their records for accuracy annually to ensure their medical records were not altered intentionally or unintentionally." Participant 3 went on to say:

> In addition to training our patients, we also have other measures of security by ensuring only the last four digits of their social security numbers or identification used to prevent an imposter from using one's identity. Due to the nature of the services rendered, we adhere to HIPAA requiring us to handle patients information privately.

Participant 5 echoed the current system, saying "that we have now had many adjustments to upkeep with changes in our society." Participant 5 also pointed out that:

> Barriers come from employees resistant to change but training is one of the tools that we rely upon to ensure employees know and understand what's needed to protect patients and their sensitive information. We must invest the time to

educate consumers on properly protecting personal and sensitive information at home in their possession which could result in prevention of exposing personal data for thieves to steal your identity.

Participant 5 provided confirmation that proper safeguard and protection of personal and sensitive data kept at peoples' residences help to prevent identity theft leading to medical identity fraud. Combined perspectives shared by participants' 1, 2, 3, and 5 confirmed and provided insights into the importance of training for employees and patients. P4 on the opposite end of the continuum arguably disconfirmed P1, P2, P3, and P5 views by not acknowledging that training employees and patients play an integral role towards the strategies to protect, safeguard, and prevent identity theft and medical identity fraud. Private and public organizations need to continuously ensure the protection of resources to improve efficiencies and delivery of services according to (Bernik, 2014).

Theme 2: Technology

Utilization of technology was the second theme emerging from the voluntary responses provided by participants during telephonic interviews. Table 3 is an illustration of three subthemes including Kiosk, Cloud and encryption software, reflected.

Table 3

Subtheme Developed from Technology

Subtheme	*N*	Participant
Kiosk or CAC	9	1, 2, 3 and 4
Cloud and off-site storage	5	1, 2, 3, 4, and 5
Encryption	5	1, 2, 3, 4, and 5

Note. *n* = frequency.

Participant 1described the Kiosk system,

> We use two components, one could be visual (by the clerk) at the front desk or it could be a Kiosk system. If they use the Kiosk, they would actually put their ID card into the system which reads the information. They would verify the information on the screen which cross-references the data from the verification perspective. We are transitioning to the Kiosk system and still in the processing stages at this time. The idea is to check-in every patient through the Kiosk system that has some built-in internal controls to help validate and verify the individual's information.

Expanding on the information on the Kiosk system, Participant 1 continued to describe the primary login process:

> The primary login process is a two-tier login system. Every employee has a Common Access Card or a card with a chip that slides into the computer. The computer reads the card and the user have to enter a pin or verification number and that validates saying that's the pin number associated with that employee. Separation of duty issues not necessarily from stealing one's identity but to ensure someone is not inappropriately billing erroneously. On the electronic health records (EHR) side of the house, we have a built-in system to protect the record. When you pull the record and pop it up on a screen, employees will be alerted that this is a restricted record do you really need access to this record. If the employee viewed a record without having the need to access that could lead to disciplinary action.

Participant 2 stated,

> We use encryption software or methods to encrypt e-mail and other data to prevent the unwarranted invasion of privacy. If someone gained unauthorized access to a computer, the information is encrypted and protected by the use of Smartcard or personal identity verification card. In other words, unauthorized access is prohibited by the use of Smartcard or PIV preventing exposure of sensitive information.

According to Participant 3, electronic records are protected by All-scripts and stored in the Cloud. All-Scripts have tight security requiring several levels of entry eliminating the need to hire an Information Technology company. Participant 3 shared that All-Script encryption was completely upgraded within the past 3 or 4 years. The utilization of Cloud computing is vital to large, medium and small businesses whereby data integrity is an important aspect of verification using a hashing algorithm, signature algorithm or hash value generated signature (Sun & Wang, 2013). Small medical practices in the state of New York could benefit from this type of information technology services as a data security protective mechanism providing reliable safeguard supporting patients' records.

Participant 4 had a different outlook on the EHR system, noting,

> I'm sure if you'll interview other healthcare professionals, a lot of people thought it would have been a great system but it's time-consuming. Right now, we're doing a transition to electronic records. In our office, we have a company that we contracted with to make the transition. I feel that no system will be perfect. To

> start the program in transition to the patient and the records is very time-consuming and tedious. A lot of physicians are in their offices hours after the data is written in a chart so we're making the transition because we have no choice. We are getting penalized by certain insurance companies for not having the electronic medical record (EHR) but that is purely a financial decision on our part because our office as well as many medical offices sat down and did the economics and found that the time spent transitioning to EHR dealing with all the other information at the end of the day you could see 4 or 5 patients during that period of time and the penalty become actually not significant. So, we're in transition and we're doing it slowly to make sure we have the right one. I'm not sure if the EHR system is best for the patients and medicine in the long run. I'm in the minority because everyone seems to think that it is best.

According to P5, in order to stay within the guidelines, "we transitioned to an electronic health record (EHR) system to eliminate the hassles of having to store and protect hard copy documents." Participant 5 went on to describe drawbacks and benefits to the system:

> I must say that the EHR system has pros and cons. For example, we are not forced to maintain hard copy documents because we transitioned to the EHR system but the down-side comes from network problems which makes it difficult and in some cases impossible to access a patient's records. Another major drawback comes from spending a few extra hours to input data into the system after patients' leave but once it's in the system documents are easier to access and that's what I enjoy.

> I also believe that if used correctly, the EHR system protects patients' SSN and other sensitive information which gives us peace of mind. We also have the ability to find out if an employee accesses a record intentionally or by mistake and when that happens, there are times when appropriate disciplinary actions occur. Our job is to protect and safeguard patient's data and I expect all of my employees to comply with the rules.

Increased escalation and growth of identity theft leading to medical identity fraud could be attributed to criminal offenses occurring in cyberspace by hackers and internal threats directly linked to employees abusing companies' resources for money (Bernik, 2014). In terms of *subtheme* d*eveloped from Technology, p*articipants' 1, 2, 3, and 5 confirm that proper safeguard and security empowers business leaders and enhanced their knowledge and ability to implement suitable protection of organizational resources and reduce direct and indirect costs. Bernik (2014) model placed emphasis on five internal costs including (a) *detection* enabling reasonable means to detect and deter crisis (b) *investigation and escalation* involving efforts that are essential to identify the source, scope, and extent of one of the numerous incidents, (c) *containment* focused on stopping or reducing threats, (d) *recovery* deals with on fixing or remediating essential business processes, and (e) *ex-post response* requires actions to minimize potential future attacks adding new technology and control systems.

P4 disconfirm P1, P2, P3, and P5 beliefs by stating "I'm not sure if the EHR system is best for the patients and medicine in the long run. I'm in the minority because everyone seems to think that it is best." Melnik (2014) confirmed P4's discontent. Melnik

stated not all physicians were satisfied with the EHR system dated back to 2013. Verbiage from survey results revealed physicians and other user satisfaction from 2010 to 2012 fell by 12%. User dissatisfaction further led to 34% claiming that EHR did not decrease workload as confirmed by P4 stating "time spent transitioning to EHR dealing with all the other information at the end of the day, you could see 4 or 5 patients during that period of time as the penalty from insurance companies become not significant."

Theme 3: Protective Measure

The protective measure was the third theme emerged from participants' responses shifting the focus to SSNs, EHR system, photo identification or picture, confidentiality agreement, and HIPAA reflected in Table 4.

Table 4

Subtheme Developed from Protective Measure

Subtheme	*N*	Participant
SSN	42	1, 2, 3, 4, and 5
EHR	21	1, 3, 4, and 5
Photo identification/picture	19	1, 2, 3, 4, and 5
Confidentiality agreement	4	4 and 5
HIPAA	3	3 and 5

Note. *n* = frequency.

According to P1, they use multiple methods to validate the data on that particular individual and also capture their insurance data and the patient gives them a picture ID and the name and social security number (SSN):

> Once they're in the system, we use the two-point identifier for each individual. A combination of both their name and date of birth or last 4 digits of the SSN and name followed by checking the full SSN matching it with what's on their ID card.

> Those are the measures used across the healthcare system to ensure that we have the right patient and the patient have the right information related to that patient and not a fraudulent person using someone's data or someone else's SSN to access care. We use multiple methods to validate the data on that particular individual and also capture their insurance data and the patient gives them a picture ID and the name and social security number. We also keep in our system patient's picture ID which has the patient information for clerks to verify the data. (P1)

Participant 2 stated, "We use encryption software or methods to encrypt e-mail and other data to prevent the unwarranted invasion of privacy." The encryption ensures that "even if someone gained unauthorized access to a computer, the information such as SSNs are encrypted and protected by the use of Smartcard or personal identity verification card" (P2). In other words, unauthorized access is prohibited by the use of Smartcard or PIV preventing exposure of sensitive information such as SSNs.

Participant 3 shared that "we attended numerous conferences for the industry that kept us abreast of all changes relating to healthcare that's handled by an EHR vendor." Participant 3 also pointed out that patients are required to provide identification with a photograph or picture before rendering services:

> Due to the nature of the services rendered, we adhere to HIPAA (Health Insurance Portability and Accountability Act) requiring us to handle patients information privately. HIPAA brought along other security measures including training staff members to ensure they understood patients' medical records should be

> safeguarded to prevent exposure of names, addresses, telephone and social security numbers. (P3)

Participant 4 also stated that patients have to show a picture ID and the appropriate insurance paper which is verified online as well as their contact information:

> If someone comes in the next time on a visit, we have the comparison with their picture ID and most likely it's a New York State Licenses which is copied and placed in their medical record. From day one, we have vendors and everyone that comes in the office including cleaning people, delivery people or anyone that works in the office has to sign a confidentiality agreement saying they won't be looking for patients' charts or removing anything.

Participant 5 stated:

> I have been in the medical field for over 25 years of my life. I remember when SSNs were used as the main identifier for each patient but over the past 15 plus years, we had to change our strategy to protect patients' information. That is one of the reasons why we follow HIPAA rules to stay within the guidelines to ensure full protection of patients' records and sensitive information. I also believe that if used correctly, the EHR system protects patients' SSN and other sensitive information which gives us peace of mind. After the information is provided, the clerk ensures that patients provide a picture or ID (New York driver's licenses) making sure it is the right person.

According to Merisalo (2014), medical identity fraud was responsible for 33% of data breaches which placed patients' at risk as HIPAA imposed $50,000 financial penalty

against health care providers from jeopardizing patients' lives. Participant 3 confirmed the applicability of HIPAA which was the main conceptual framework for this study. P3 confirmed by stating "due to the nature of the services rendered, we adhere to HIPAA (Health Insurance Portability and Accountability Act) requiring us to handle patients information privately." Participant 5 also confirmed applicability noting:

> I worked in the medical field for 25 years and remember when SSNs were used as the main identifier for patients. During the past 15 plus years, we changed our strategy and protected patients' information resulting to one of the reasons why we follow HIPAA rules to stay within the guidelines to ensure full protection of patients' records and sensitive information.

Participants 1, 2, 3, 4, and 5 confirmed protection of SSNs coupled with safety and security for patients through implementation of other protective measures from using photograph and identification including New York states driver's licenses. Perspectives from the five participants' confirmed that adoption of standards for storing and managing leads to patient-centered health care for patients that enhanced quality and safety (Ben-Zion, Pliskin, & Fink, 2014).

Theme 4: Safeguarding PII data

Safeguarding PII data was the fourth major them emerging from participants' perspectives shared during telephonic interviews. Table 5 illustrates the subtheme, frequency, and participant positions on the topic.

Table 5

Subtheme Developed from Safeguarding PII Data

Subtheme	*N*	Participant
Safeguarding PII data	11	1, 2, 3, 4, and 5

Note. *n* = frequency.

Participant 1 stated that training involves care and safeguarding of personally identifiable information such as social security numbers, home-addresses, patients' disability, and the nature of their disability, ensuring pertinent data is properly safeguarded. P1 shared that

> When the patient comes into the healthcare system, they are met by the eligibility clerk that will capture their Personal Identifiable Information (PII) and verify it. When patient use the Kiosk system, they would verify the PII information on the screen which cross-references the data from the verification perspective. Those are the measures that we take across the healthcare system to ensure that we have the right patient and the patient have the right PII information related to that patient and not a fraudulent person using someone's information or someone else's SSN to access care.

According to Participant 2, the majority of the procedures associated with safeguarding data are established by the Office of Information Technology department and the Freedom of Information Act section describing what data may be releasable. "The use of encryption and training prevents unauthorized access to sensitive information

or documentation. The current safeguards in-place prevent such infractions from happening" (P2).

Participant 3 stated,

> We also provide training to patients to ensure proper handling and safeguard of their health records and personally identifiable information (PII). In fact, when MIF became prevalent, we advised patients on what they could be susceptible to if his/her PII was not properly protected. In addition to training our patients, we also have other measures of security by ensuring only the last four digits of their social security numbers or identification used to prevent an imposter from using one's identity.

According to Participant 4,

> We have vendors and everyone that comes in the office including cleaning people, delivery people or anyone that works in the office has to sign a confidentiality agreement saying they won't be looking for patients' charts or removing anything. The charts are locked up at the end of the day and we have a security officer that's responsible for keeping us up-to-date on everything in the office to prevent people from getting access to the records. We don't give information over the phone. People would come into the office saying to whom they would like to discuss their medical record. If someone calls and said they want to discuss Mrs. Smith condition, they've to identify themselves. If the person is not properly identified such as the spouse or parent, we do not release or give them any information without proper authorization.

Participant 5 stated that barriers also come from employees who are resistant to change but "training is one of the tools that we rely upon to ensure employees know and understand what's needed to protect patients and their sensitive information." Participant 5 went on to say:

> I know that the strategies we use prevent us from having to worry about identity theft because SSNs and other sensitive patient's information are always safeguarded during the day and after hours. I also believe that if used correctly, the EHR system protects patients' SSN and other sensitive information which gives us peace of mind.

Findings and the Conceptual Framework

Healthcare leaders from small medical practices were the target audience that resulted in confirmation of the four conceptual frameworks for this study. For example, Participant 1 and Participant 5 shared two incidents that provided confirmation for three conceptual framework theories in this study (a) routine activity theory, (b) theory of rational behavior, and (c) rational choice theory. Participant 1 talked about an individual that stole his brother identity, used his insurance coverage and received healthcare services under his brother's name. Over time the imposter visited another medical facility to get additional care and was caught due to the stringent strategies in place to catch imposters. Participant 5 stated, "one of my former employees committed fraud by using my physician identifier by calling a few pharmacies in New York and ordered prescription drugs." When P5 realized what happened, the employee was fired and P5 later pressed charges against that person. As P5 stated, changes in the New York state

law today, made it almost impossible “for an employee to call-in prescriptions under my name since only physicians could call-in prescriptions today.” P5 noted, “I believe the systems in-place prevent imposters from visiting my office to get healthcare under another person's name.” Perspectives shared by Participant 1 and Participant 5, provided confirmation for routine activity theory, working under the assumption that people intentionally make rational choices to commit crimes as in the case with sibling and employee made the rational choice and committed the crimes.

The theory of rational behavior stated that some people make conscious decisions to commit crimes while others refrain from criminal misconduct. Once again, an imposter stealing his brother’s personal information and received healthcare care followed by the employee that used the physician identifier and illegally ordered prescriptions made conscious decisions and committed the crimes instead of refraining from the criminal misconduct. The rational choice theory stated people commit crimes by weighing the odds against the cost of not getting captured or punished. Both individuals’ actions in the cases above confirmed they weighed the odds against the cost of not getting captured or punished. For example, the sibling that stole his brother’s identity and received healthcare illegally and decided to visit another facility to evade capture but ironically he did not realize that his brother normally received care from that facility. In terms of the employee that used the physician’s identifier, she did not realize that New York lawmakers changed the system requiring only physicians to call-in prescriptions alerting the physician that the employee falsely ordered prescriptions.

Perspectives shared by P1 confirmed the devastation of identity theft and medical identity fraud. Even though only five people participated in this study, one of the five experienced identity theft that occurred between two brothers. P1 testimony confirmed and provided credence to three of the four conceptual frameworks that included: (a) routine activity theory (RAT) whereby the imposter intentionally stole his brother's personal data and illegally acquired healthcare services, (b) theory of rational addiction behavior (TORB) whereby an imposter made a conscious decision and committed a crime instead of refraining from doing the illegal activity, and (c) rational choice theory (RCT) as the imposter made a rational choice and committed a crime against his brother for personal gain.

Participant 5 statements regarding a former employee's theft using the physician's identifier and purchased prescription drugs confirmed about the devastation of identity theft and testimony also aligned with RCT, TORB, and RCT theories. A portion of P5 testimony that extended knowledge alerting that of New York State's officials changed the law that made it almost impossible for an employee to steal prescriptions under physicians' names because only physicians allowed to call-in prescriptions today.

Perspectives shared by Participant 1 and Participant 5 provided confirmation of the main conceptual theory HIPAA. Participant 3 stated,

> Due to the nature of the services rendered, we adhere to HIPAA (Health Insurance Portability and Accountability Act) requiring us to handle patients information privately. We put several measures in-place starting with transitioning from paper chart to the Electronic Health Records. HIPAA brought along other security

> measures including training staff members to ensure they understood patients' medical records should be safeguarded to prevent exposure of names, addresses, telephone and social security numbers.

Finally, Participant 5 stated that his organization follows HIPAA rules to stay within the guidelines to ensure full protection of patients' records and sensitive information, which directly ties to the conceptual framework for this study.

Applications to Professional Practice

In today's economic climate, healthcare leaders faced numerous challenges that include identity theft and medical identity fraud. High employee turnover rate in the healthcare arena could be a contributing factor to theft and fraud. Shortage of healthcare clinicians might be detrimental to the medical industry because losing experienced professionals with the corporate knowledge and capability could be the key to safeguarding and protecting patients' PII (Alshanbri et al., 2015). Losing talented clinicians without the opportunity to transfer knowledge forces organizational leaders to train new employees.

According to McManus and Mosca (2015), employee turnover resulted to $10 billion in losses that stemmed from lack of appreciation. Healthcare leaders need to address the high turnover rate issue and adopt long-term solutions by implementing successful strategies used to reduce IT leading to MIF for better performance increasing the chances of survivability in a volatile industry. The absence of effective strategies to reduce IT and MIF would drastically decrease the chances for medical facilities to survive in today's competitive environment and remain solvent in the future.

Healthcare leaders from large, medium, and small medical facilities should apply the findings captured in this study to reduce identity theft and medical identity fraud to improve business performance, especially those leaders practicing in the state of New York. Since the medical industry became volatile from high employees turnover, healthcare leaders should adopt effective retention strategies to retain top performers and prevent loss of revenue. P1 through P5 stressed the need to incessantly safeguard and protect patients' records and PII to prevent the unwarranted invasion of privacy followed by maintaining the confidentiality of peoples' personal information. A change in direction by healthcare leaders could build a culture of trust and demonstrate appreciation for employees preventing high turnover and better safeguard for patients' records and PII.

Implications for Social Change

When working with people, communities, organizations, cultures, and societies, social change was predicated on *learning,* which results in a change in behavior provoking resistance (Reeler, 2015). According to Reeler (2015), social change does not necessarily occur merely by cause and effect but triggered by inner and outer influences deemed by society. Medical identity fraud is growing faster than conventional identity theft threatening patients' identities by falsifying patients' records causing malpractice claims against physicians (Satter, 2014). Financial effects of this crime led to losses totaling $9 billion in the United States followed by $110 billion worldwide affecting 500 million victims each year equating to 18 persons per second (Demarest, 2014). When it comes to implications to social change, the overarching premise would stem from curtailing or eradicating identity theft and medical identity fraud. Identity theft crises set

the stage for transformative change by adopting new ideas, values, and beliefs to eliminate imposters' footprint forcing humanity to change (Reeler, 2016) to fight against one of the most heinous crimes and prevent personal or financial gain imposed by imposters.

The real social change was predicated on renewed mindsets and sound government intervention holding criminals accountable for their actions by responding to the public outcry from victims of medical identity fraud. Keehan et al. (2017) projected between 2016 to 2025 national health expenditures growth from inflation will average 5.6% outpacing the gross domestic product by 1.2%, while economical healthcare escalated by 18% in 2015 with the expectation to climb to 20% by 2025. What is interesting is that Medicaid and private healthcare insurance were estimated to decrease to 3.7% in 2016 and 2017 in comparison to 12% increase during 2014 and 10% growth back in 2015. Following in 2018, the projection for Medicare and Medicaid projection will grow rapidly than private health insurance averaging 8% for 2020 through 2025 (Keehan et al., 2017).

Findings expressed by scholars could have a profound effect on healthcare delivery services, depleting profits for medical facilities, which would impact society as a whole. The expansion and growth of Medicare and Medicaid would make both programs a more lucrative target for thieves to commit incessant fraud and abuse. During telephonic interviews, P1 alerted about waste and unnecessary spending in the healthcare system expressing belief that the Federal government needs to adopt more stringent penalties to help eradicate this heinous crime. I believe that if health care fraud continues

the rapid growth, it would lead to major deficits resulting in declining budgets for future healthcare delivery services with crippling effects across the medical industry. Findings from this study may ameliorate these effects and contribute to social change through improved healthcare services and reduced medical costs, leading to more affordable healthcare.

Recommendations for Action

Recommendations for action are addresses to healthcare leaders from small, medium, and large medical practices including the Department of Veterans' Affairs followed by leaders across all industries including the branches of the military. The issues stemming from identity theft leading to medical identity fraud affects humanity as a whole. During this study, it was determined that identity theft and medical identity fraud occurs in organizations and peoples' residences.

After publishing this dissertation, I will start disseminating results from this study by e-mails to the five participants who shared their perspectives and the 10 potential participants who could not participate in interviews due to conflicting schedules. Additionally, I will contact small, medium, and large medical practices, the Internal Revenue Services, and Social Security Administration and provide a copy via e-mail to members who express an interest to review the results from this study. Based on the 100% success rate from the strategies five participants used in New York, I endorsed adapting those effective strategies for (a) healthcare leaders in organizations, (b) identity theft victims, and (c) consumers. For a better understanding, here are the details:

Organizations

The initial recommended action is directed to healthcare leaders to ensure employees are trained to properly safeguard patients' records to prevent the unwarranted invasion of privacy and stop thieves from stealing PII and sensitive data. Also, patients should be educated on reviewing their records for inconsistencies and checking to see if personal information was altered. Collectively, Participants 1, 2, 3, and 5 stated training for employees 11 times while participants 1, 3, and 5 mentioned it a total of three times to educate patients to examine their records for mistakes or alteration annually or on an ad-hoc basis if needed.

The next recommended action is directed to leaders in health care, the Department of Veterans' Affairs, and other industries because identity theft is a crime of opportunity occurring in all organizations. Based on the strategies shared by P3 and P5, health care entities should adopt utilization of HIPAA law because it ensured patients have clearly defined rights and access to their medical records. Adopting HIPAA should also ensure confidentiality, integrity, and availability of sensitive data as confirmed below:

Participant 3 stated, "due to the nature of the services rendered, we adhere to HIPAA standards requiring us to handle patients' information privately." HIPAA brought along other security measures including staff members to ensure they understood patients' medical records should be safeguarded to prevent exposure of names, addresses, telephone, and social security numbers.

Participant 5 shared that SSNs were once used as the main identifier for each patient but that over the years the strategy has needed to change in order to better protect

participants. Participant 5 believed “that if used correctly, the EHR system protects patients' SSNs and other sensitive data which gives us peace of mind.” Adoption of HIPAA led to confidentiality, integrity, and availability of sensitive data providing safeguards for PHI. Enabling separation of duties ensured healthcare providers, physicians, nurses, insurers, and other stakeholders afforded access only on a need-to-know basis to secure patients’ privacy (Mohammed & Mariani, 2014).

Protective measure is this recommended action directed to healthcare leaders in small, medium, and large medical practices. Protective measures calls for utilizing encryption software to safeguard and protect records being transmitted electronically in cyberspace whereby Participants 1, 2, 3, 4, and 5 frequencies totaled 42 times. In terms of validation tools, P1 used Kiosk and identification (ID) while P2, P3, and P4 used ID including New York State Drivers’ License.

Utilization of the EHR is another recommended action as confirmed by P1, 2, 3, and 5 felt that its adoption was a great tool ensuring added security than using charts. Despite their belief, P4 felt that the system was too time-consuming as it took time away from providing healthcare delivery services from patients.

The following recommended action is the need for continued protection of SSNs as confirmed by Participant 1, 2, 3, 4, and 5 frequencies totaling 42 times. For this reason, training and education should couple with proper utilization of EHR to safeguard patients’ PII data. Full protection of SSN is critical to the prevention of identity theft and medical identity fraud.

The following recommendation is addressed to the Chairman of the Joint Chiefs of Staff followed by the Chief of Staff of the Army, Chief of the Staff of the Air Force, and the Chief of Naval Operations. Four-Star General Officers need to revisit and change portions of the 1949 Geneva Conventions rules stating military personnel needs to provide SSN when captured or serving as a prisoner of war (POW). According to the Articles of the Code of Conduct, Article V stated that POW and missing-in-action (MIA) military personnel are required to provide name, rank, date of birth (DOB), and SSN to their captors (Ratner, 2009). While serving in the Air Force, military members were and still required remaining the accepted rules to provide DOB and SSN to captors. Based on changes in our new World Order with Al-Qaida and other terrorists groups, military General Officers should revisit Article 5 and change the language to read "POW or MIA personnel are required to provide name and rank to captors" omitting the antiquated requirement to provide DOB and SSN.

Service men and women should no longer be compelled to provide personal and sensitive information. They could fall prey and become victims of the identity theft and medical identity theft and held liable for unscrupulous thefts committed by others. Government officials need to remove the provision for providing DOB and SSN because others could benefit from the antiquated flaw of the past by committing identity theft against service members in captivity. A second point worth mentioning, once government officials realize military personnel fall prey as a POW or MIA, fraud alerts should be initiated for the service member being captured to prevent others from assuming the

victim's identity. Adoption of fraud alerts should result in raising red flags if there is an attempt to use, steal, or captured victims' identities.

Identity Theft Victims

The next recommended action is directed to victims of identity theft. Victims of identity theft should take the first step and file a police report upon realizing he or she became a victim to confirm that a crime was committed against them. The police report would serve as the official source document informing other agencies about the criminal activity levied against the victim. Subsequently, victims should provide a copy of the police report to the three credit bureaus—Experian, Transunion, and Equifax—alerting them to the problem.

Identity theft incessantly raises major concern, costing business owners, and members of society billions of dollars resulting in greater attention from public policy makers (Betz et al., 2012). According to Demshock (2016), identity theft crises occur numerous ways including mail theft, dumpster diving, credit card theft, skimming, phishing followed by tax return fraud as imposters filed for tax refunds to the Internal Revenue Service under their victims' names. Consequences from identity theft have resulted to the inability to obtain loans, rent housing, or gain employment as the destruction to repair damage credit take years to fix through the legal system (Demshock, 2016). People should become more self-conscious as consumers need to adopt new protective measures to prevent from becoming victims of identity theft.

Consumers

The next recommended action focus on added protection for adults, children, and babies. As identity theft became a crime of opportunity, I encourage consumers to subscribe to credit monitoring companies that are linked to the three credit bureaus. Credit monitoring agencies served as independent entities with oversight authority providing identity protection by monitoring peoples' credit files guarding against suspicious activities across the Internet and other public places.

Costco Wholesale Company extends credit monitoring protection totaling $8.95 a month for adults and $2.99 a month for children and babies for Executive members. Costs for Costco Gold star members totaled $13.99 a month, and $3.99 per month for children and babies. Life-lock is another company that provides credit monitoring protection with price starting at $9.99 a month for Life-lock standard followed by Life-lock advantage totaling $19.99 a month, and Life-lock Ultimate Plus package costing $29.99 per month. Identity Guard is the third company for inclusion into this study as the cost for the Identity Guard with Watson package totaled $19.99 per month followed by Total Protection Identity Guard for $19.99 a month and the Identity Guard Platinum package totaling $24.99 per month.

There are other companies in addition to the three main credit bureaus, including Bank of America and Citibank that offer similar protection with competitive rates. Regardless of the company, consumers will be alerted when suspicious or other activities occur under their names and afforded online access to view credit reports followed by the ability to check credit score, and other credit analyzer tools. I believe that the minimal

costs per month for monitoring protective services is money well-spent compare to hundreds or thousands of dollars stolen by thieves or imposters inflicting punishment against victims leaving them liable for charges they did not incur.

Monitoring protection is another recommended action resulting to a compelling need for parents and guardians to purchase credit monitoring protection for children and babies even though they are not of legal age to enter the workforce. Children and especially babies became a lucrative target. Thieves realize they could use (i.e., children and babies' identities) without fear of being captured based on clean credit history since they are too young to established credit (Betz et al., 2012). Children and babies are at the mercy of identity thieves putting their identities at great risk. If they do not get the proper protection they will eventually become victims of identity theft and medical identity fraud leaving them liable for financial losses and personal liability imposed by thieves and imposters.

Recommend that Internet users seek assistance from computer experts to properly install and configure firewall, antivirus, and antispyware on home computers before surfing the Internet to prevent hackers and intruders from gaining unauthorized access to their computers. The Internet is a shopping playground that benefits billions of consumers but it also became a safe-haven for hackers. Insurmountable Internet growth evolved to a collection of technologies satisfying the community needs that started with 394 million Internet users in 2000; 1.02 billion in 2005; 2.03 billion in 2010, and 2.92 billion dated back to 2014 (Statistic, 2015).

The installation of firewall works directly with the computer operating system providing added protection preventing hackers from gaining access to a person's computer. Even though firewall prevents hackers from gaining illegal access if disabled intentionally or unintentionally computers could be left dangerously exposed to the Internet (Al-Shaer, 2014) allowing hackers to high-jack consumers' computers and steal information. Installation of antivirus software is critical for safeguarding computers prior to accessing the Internet. A few well-known antivirus software vendors are Norton, McAfee, and Symantec being sold on today's market.

Antivirus is a major component for identifying, detecting, preventing, isolating, eliminating, and recovering documents if corrupted (Al-Shaer, 2014). Specific scanning is the first line of defense virus definitions and signatures downloaded by antivirus updates. Its main purpose protects against malicious logic code. Users can take corrective actions and prevent viruses from spreading to all files infecting the entire computer hard drives (Rao & Navak, 2014).

Installation of antispyware software is a critical protection against spam software as it runs in the computer memory preventing hackers or intruders and malicious software from accessing consumers' computers (Rao, & Navak, 2014). Antivirus software works similar to a doorkeeper that uses a by-name list to see if the person's name was on the list. If the name appears, the doorkeeper allowed access but disallow access if the name was not included on the list. Similarly to the doorkeeper concept, antispyware will disallow access to intruders if they did not obtain the right permission to gain access.

Further recommendation calls for consumers to utilize strong passwords on home computers. Passwords that easy for users to remember but difficult for hackers to break provides maximum security and protection preventing work stoppage and destruction to computers. Users' passwords should contain a combination of 12 to 16 upper and lower case letters, numbers, and symbols. For example, passwords with six characters with only uppercase letters or lower case letters took hackers 32 seconds as the success rate for hackers ranged from 62% to 90% that took less than 1 hour (Woollaston, 2013). Using the combination of 12 to 16 upper and lower case letters, numbers and symbols make it difficult for a hacker to combine a dictionary attack with a brute-force attack preventing unauthorized access to peoples' computers across the Internet (Woollaston, 2013). For example, Shakespeare's plays: To be or not to be that is the question combined with symbols could become this strong password: #2bON2bTiTq@.

The following recommended action calls for government officials to educate consumers on protecting private and sensitive data kept in their possession at home to prevent thieves or imposters from stealing personal data. For a better understanding of the devastation about identity theft, Figure 6 shows a graphical display detailing complaints relating to identity theft crimes.

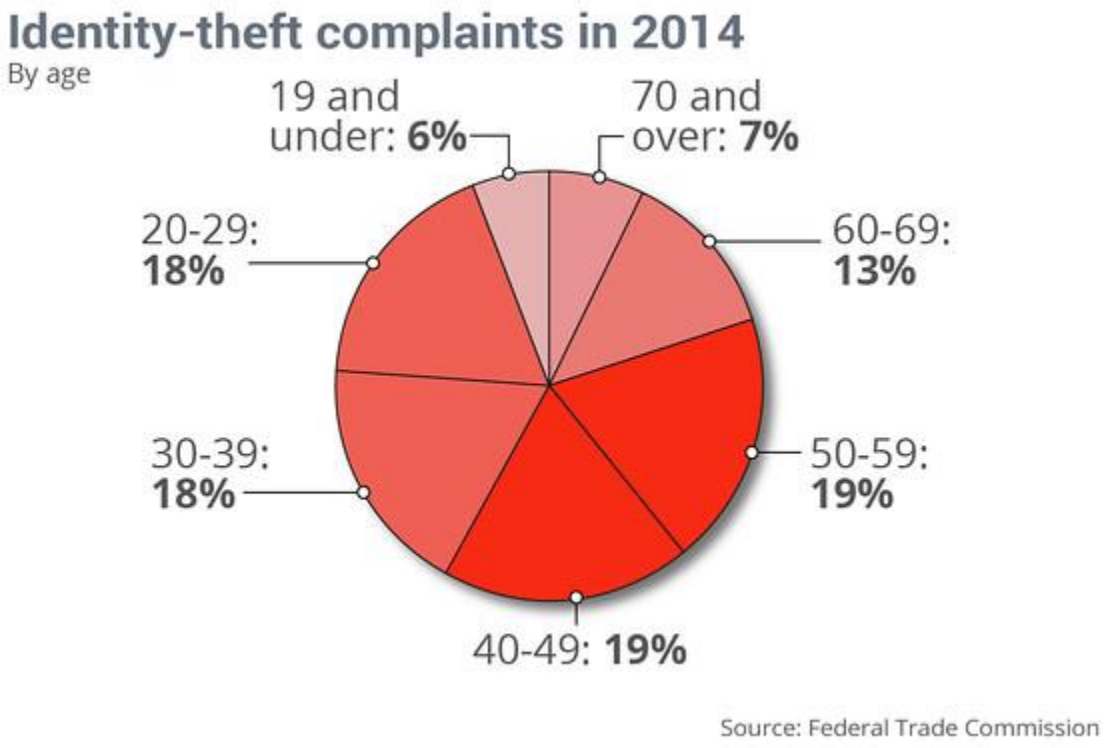

Figure 6. Identity theft complaints by aged group (Federal Trade Commission, 2014).

Data in Figure 6 highlights how identity thieves victimized individuals in different age groups. Individuals between ages 19 and below became victims of identity theft totaling 6% followed by 18% for persons between 20 to 29-years-old. Individuals in ages 30-39 totaled 18%; 19% for persons between ages 40-49 followed by people between ages 60-69 and 70 and above totaling 13% and 7% respectively (Federal Trade Commission, 2014). Widespread complaints against different age groups in 2014 showed the significance of this rapid growth dealing with the identity theft problems.

Observation leading to a recommendation: Women carrying pocket-books and men carry messenger boy-bags have a tendency to place them into the top portion of

carts. The innocent act occurs while shopping for household and other goods in Supermarkets, Target, and other businesses that provide carts.

The final recommended action calls for women with handbags and men carrying body-bags to refrain from placing them in the top portion of shopping carts and walk-away to examine goods and products leaving their belongings unattended as they are caught up in the moment shopping. I am making this recommendation because two or more thieves could create a diversion scheme and steal women's pocket-books or men's boy-bags with personal and sensitive information (including driver's license, government identification, and possibly social security cards) to prevent from becoming victims of identity theft. During the month of October 2017, I observed 46 women and two men walk away from shopping carts leaving pocket-books and messenger boy-bags unattended while shopping in Costco and Target. The innocent mistake of leaving personal belongings to examine goods and products while shopping could have a devastating effect because it could lead to identity theft followed by medical identity fraud.

Recommendations for Further Research

This study regarding strategies to prevent and reduce medical identity theft resulting in medical fraud could have significant importance to business entities across all industries. Financial losses impersonators inflicted by committing medical identity fraud threatened survivability and sustainability of the healthcare system. Medical identity fraud-plagued one-third or 33% of computer network breaches resulting to 91% of healthcare facilities experienced at least one breach while 79% had two or more breaches

(Carlson et al., 2014). Recommend further studies in other regions of the United States and overseas to capture a better sight-picture of the devastation and share new insights regarding how identity theft led to medical identity fraud. Results from this study were limited because I only collected data from healthcare leaders within the state of New York. According to Madsen (2013), limitations are constraints or flaws levying restrictions on scholars' ability to assess problems or issues. For example, results captured in this study came from a small sample size by conducting telephonic interviews with healthcare leaders from five medical practices only in the state of New York.

Further limitation came from conducting telephonic instead of face-to-face interviews resulting to a disadvantage from the inability to observe participants' facial expressions and body language to determine honesty or untruthfulness. Participants' dishonest feedback affects the validity, reliability, and credibility of information shared resulting to inaccurate representation of their perspectives and experiences according to (Madsen, 2013). Based on incessant challenges in the healthcare field, there is still a compelling need for other researchers to explore the strategies healthcare leaders use to reduce identity theft and medical identity fraud beyond the borders of New York to improve performance, increase profit, and strengthen the healthcare industry.

Reflections

The overarching goal of this qualitative multiple case study explored the strategies some medical practice healthcare leaders used to reduce identity and medical identity fraud to improve business performance. I discovered during this journey that persistence resulted in progress despite minor and major setbacks during different stages

of the Doctor of Business Administration process towards completion of this final project. For example, one-on-one telephonic interviews with participants were challenging but I eliminated personal biases by reverting to the rules established in the interview protocol (see Appendix C). During interview sessions, I was silent as participants shared their perspectives and kept the focus on capturing their unbiased opinions.

Collection of data captured from participants coupled with the analysis of responses enabled me to identity the successful strategies some healthcare leaders used to prevent identity theft and medical identify fraud and improve business performance. Before soliciting participants to conduct telephonic interviews, I felt it would be easy to find suitable candidates to participate in this study but later changed my thinking as it became more difficult than expected. After IRB approval, I reached out to 15 potential participants and 10 agreed to telephonic interviews. From the remaining 10, five became inundated with work and were unavailable to support the effort leaving five participants' for interviews. From experience, time management played a key role in this study that enabled me to remain squarely on track towards completion of the project.

In soliciting potential candidates, individuals shared concerns about identities being exposed since the identity theft crisis leading to medical identity fraud was a sensitive subject. Throughout the collection process, I ensured that information provided via e-mails, and telephonic interviews remained confidential to protect participants' identities including names, organizations, and recorded data. Findings from this study

may result in a major contributing factor to prevent or cease identity theft which remained a heartless crime of opportunity claiming billions of new victims annually.

Conclusion

Thieves and imposters committed identity theft and medical identity fraud and incessantly affected humanity on a global scale. Government officials from different countries need to collaborate and make it easier to extradite thieves when captured. The focus today is to find solutions tomorrow to eradicate the identity theft crises to protect our future. Permit this researcher to speak in three voices moving forward as destruction from identity fraud spiraling out of control demoralizing billion of victims while Federal government officials continue to lose the battle.

First, there must be a total collaboration between Congressional lawmakers, business leaders and consumers as the identity theft issue is quite systemic. For example, even if business leaders and employees in the workplace provided 100% protection and safeguarded peoples' sensitive data, identity theft and medical identity fraud could still happen if consumers lack the skills to safeguard personal data kept at home. Training for professionals in the workplace to properly handle patients' sensitive data is important but from a business perspective, consumers must also be educated to protect and safeguard personal information in their possession. Most consumers are not cognizant of the ruins from the identity theft crisis and must be armed with practical tools to securely safeguard and protect personal data in their possession. Perspectives capture from participants' telephonic interviews should also lead to new solutions for healthcare leaders and leaders

in all industries to adopt and combat against one of the most heinous crimes as a benefit to society as a whole resulting to the second voice.

Second, consumers on the home-front should abstain from releasing personal and sensitive data and only share with government officials and professionals having a need to perform business transactions. People at home must protect SSNs for adults, children, and babies because added security would stop illegal activities. Consumers need to use strong passwords; ensure firewalls, spyware, and antivirus protection installed on computers, safeguard regular mail by purchasing mailboxes with locks, and shred important documents upon expiration. Abstaining from using free public wireless fidelity (Wi-Fi) in restaurants, hotels, conferences, and Airports would prevent thieves from capturing peoples' passwords and financial data masking criminals' intent by offering free Wi-Fi. Demshock (2016) alerted that people should check credit reports at least quarterly to identify discrepancies and pinpoint, illegal activities levied against them leading to the third voice.

Third, government officials of all nations should set-aside differences and work together and champion the effort to capture criminals and bring them to justice. At this juncture, I am introducing a new sting operation titled: Operation Spoon-Feeding for law enforcement officials. Operation spoon-feed would enable law-enforcement or task force teams to spoon-feed criminals with fake SSNs, and date of births in control environments. Once thieves use the information, law-enforcement officials would get an alert notifying the location where the crime was committed. Enforcement officials from the Federal Bureau of Investigations, Central Intelligence Agency followed by local and

State Police could play critical roles by arresting criminals and bring them to justice. Operation Spoon-Feeding tactics could serve as a catalyst to stop thieves and imposters and serve as the Strategies to Prevent and Reduce Medical Identity Theft Resulting in Medical Fraud. I truly believe that many of the strategies and perspectives shared by healthcare leaders during telephonic interviews coupled with recommendations would help reduce medical identity fraud. The problem members of society face today is not *if* but *when* a new citizen will become the next victim of identity theft. These findings from this study could help to ameliorate this possibility and provide improved healthcare services and reduced medical costs, which could lead to more affordable healthcare.

References

Agrawal, S., & Budetti, P. (2012). Physician medical identity theft. *Journal of the American Medical Association*, *307*, 459-460. doi:10.1001/jama.2012.78

Agris, J. L. (2014). Extending the minimum necessary standard to uses and disclosures for treatment. *The Journal of Law, Medicine & Ethics*, *42*(2), 263–267. doi:10.1111/jlme.12140

Al-Shaer, E. (2014). Dynamic firewall configuration optimization. Automated Firewall Analytics, 95–127. doi:10.1007/978-3-319-10371-6_5

Alshanbri, N., Khalfan, M., Noor, M., Dutta, D., Zhang, K., & Maqsood, T. (2015). Employees' turnover, knowledge management and human resource management: A case of Nitaqat program. *International Journal of Social Science and Humanity, 5*(8), 701-706. doi:10.7763/ijssh.2015.v5.543

Amigorena, F. (2014). The threat from within: how to start taking internal security more seriously. *Computer Fraud and Security*, *7*, 5-7. doi:10.1016/s1361-insider

Anandarajan, M., D'Ovidio, R., & Jenkins, A. (2013). Safeguarding consumers against identity-related fraud: Examining data breach notification legislation through the lens of routine activities theory. *International Data Privacy Law*, *3*(1), 51–60. doi:10.1093/idpl/ips035

Applebaum, M. (2012). Phenomenological psychological research as science. *Journal of Phenomenological Psychology*, *43*(1), 36-72. doi:10.1163/156916212X632952

Ball, K. (2010). Data protection in the outsourced call centre: An exploratory case study. *Human Resource Management Journal, 20*, 294-310. doi:10.1111/j.1748-8583.2010.00129.x

Bamrama, A., Singh, G., & Bhatt, M. (2013). Cyber-attacks and defense strategies in India: An empirical assessment of banking sector. *International Journal of Cyber Criminology, 7*(1), 49–61. doi:10.2139/ssrn.2488413

Barnham, C. (2015). Quantitative and qualitative research: Perceptual foundations. *International Journal of Market Research*, *57*(6). doi:10.2501/IJMR-2015-070.

Barry, A. E., Chaney, B., Piazza-Gardner, A. K., & Chavarria, E. A. (2014). Validity and reliability reporting practices in the field of health education and behavior: A review of seven journals. *Health Education & Behavior*, *41*(1), 12–18. doi:10.1177/1090198113483139

Bartoska, J., & Subrt, T. (2012). The effect of human agent in project management. *Central European Journal of Operations Research, 20*(3), 369-382. doi:10.1007/s10100-011-0209-4

Baškarada, S., & Koronios, A. (2014). A critical success factor framework for information. *Quality Management. Information Systems Management*, *31*(4), 276–295. doi:10.1080/10580530.2014.958023

Bazzoli, G. J., Fareed, N., & Waters, T. M. (2014). Hospital financial performance in the recent recession and implications for institutions that remains financially weak. *Health Affairs, 33*, 739-745. doi:10.1377/hlthaff.2013.0988

Ben-Zion, R., Pliskin, N., & Fink, L. (2014). Critical success factors for adoption of electronic health record systems: Literature review and perspective analysis. *Information Systems Management*, 31, 296-312 doi: 10.1080/10580530.2014.958024

Bernard, H. R. (2013). *Social research methods: Qualitative and quantitative approaches* (2nd ed.). Thousand Oaks, CA: Sage Publications, Inc.

Bernik, I. (2014). Cybercrime: The cost of investments into protection. *Journal of Criminal Justice & Security*, *16*(2), 105–116. Retrieved from https://www.fvv.um.si/rV/arhiv/2014-2/01_Bernik.pdf

Betz, A., Gudmunson, C. G., & Hong, G. S. (2012). The recovery experiences of child identity theft victims: Preliminary results. *Consumer Interests Annual, 58,* 1. Retrieved from http://lib.dr.iastate.edu/cgi/

Bhatti, Y., Gørtz, M., & Pedersen, L. H. (2015). The causal effect of profound organizational change when job insecurity is low--a quasi-experiment analyzing municipal mergers. *Journal of Public Administration Research and Theory*, *25*(4), 1185–1220. doi:10.1093/jopart/muv006

Birley, G., & Moreland, N. (2014). *A practical guide to academic research*. New York, NY: Routledge.

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member Checking: A tool to enhance trustworthiness or merely a nod to validation. *Qualitative Health Research*, *26*(13), 1802–1811. doi:10.1177/1049732316654870

Brayda, W. C., & Boyce, T. D. (2014). So you really want to interview me?: Navigating "sensitive" qualitative research interviewing. *International Journal of Qualitative Methods, 13*(1), 318–334. doi:10.1177/160940691401300115

Bristol, S. T., & Hicks, R. W. (2014). Protecting boundaries of consent in clinical research: Implications for improvement. *Nursing Ethics, 21*(1), 16-27. doi:10.1177/0969733013487190

Brody, R. G., Haynes, C. M., & Mejia, H. (2014). Income tax return scams and identity theft. *Accounting and Finance Research, 3*(1), 90. doi:10.5430/afr.v3n1p90

Brutus, S., Aguinis, H., & Wassmer, U. (2013). Self-reported limitations and future directions in scholarly reports: Analysis and recommendations. *Journal of Management, 39*, 48-75. doi:10.1177/0149206312455245

Burns, R., & Peterson, Z. (2010). Security constructs for regulatory-compliant storage. *Communications of the Association for Computing Machinery, 53*(1), 126-130. doi:10.1145/1629175.1629206

Butler, K. H. (2016). Stark law reform: Is it time? *Journal of Health Care Compliance, November–December*, 5-14. Retrieved from http://www.greensfelder.com/media/event/247_Butler-StarkLaw-JHCC1112-16.pdf

Campbell, D. T., & Stanley, J. C. (2010). *Experimental and quasi-experimental designs for research*. Mason, OH: Cengage Learning.

Carlson, M., Lewis, K., & Nelson, W. (2014). Using policy intervention to identify financial stress. *International Journal of Finance & Economics*, *19*(1), 59-72. doi:10.1002/ijfe.1482

Caplan, N. (2013). Cyber war: The challenge to national security. *Global Security Studies*, *4*(1), 93-115. Retrieved from http://globalsecuritystudies.com

Champion, D. R. (2011). White-collar crimes and organizational offending: An integral approach. *International Journal of Business, Humanities and Technology*, *1*(3), 34-45. Retrieved from http://www.ijbhtnet.com/journals

Chittem, M. (2014). Understanding coping with cancer: How can qualitative research help? *Journal of Cancer Research and Therapeutics*, *10*(1), 6-10. doi:10.4103/0973-1482.131328

Cliff, G. (2015). Cybercrime @ City Hall. *Public Management*, 97(2) 6-11. Retrieved from https://icma.org/articles/cybercrime-city-hall

Collins, C. S., & Cooper, J. E. (2014). Emotional intelligence and the qualitative researcher. *International Journal of Qualitative Methods*, *13*, 88-103. Retrieved from http://ejournals.library.ualberta.ca/index.php/IJQM/index

Conkle, A., Wilson, M., & Sands, D. (2015). A digital utility imperative: Protecting your customer data. *POWERGRID International*. Retrieved from http://www.free trade magazinesource.com/40-2048825142/description.aspx

Connelly, B. S., Sackett, P. R., & Waters, S. D. (2013). Balancing treatment and control groups in quasi-experiments: An introduction to propensity scoring. *Personnel Psychology*, *66*(2), 407–442. doi:10.1111/peps.12020

Crabtree, A., Chamberlain, A., Grinter, R., Jones, M., Rodden, T., & Rogers, Y. (2013). Introduction to the special issue of "The Turn to the Wild." *ACM Transactions on Computer-Human Interaction, 20*(3), 1-4. doi:10.1145/2491500.2491591

Creely, E. (2016). "Understanding things from within". A Husserlian phenomenological approach to doing educational research and inquiring about learning. *International Journal of Research and Method in Education*, 1–19. doi:10.1080/1743727x.2016.1182482

Cugini, M. (2015). Successfully navigating the human subjects' approval process. *American Dental Hygienists Association, 89*(1), 54-56. Retrieved from http://www.jdh.adha.org/content/89/suppl_1/54.full

Custer, W. S. (2016). Health care cost inflation in the next decade. *Journal of Financial Service Professionals, 70*(1), 37-39. Retrieved from http://www.financialpro.org/pubs/journal_index.cfm

Daraiseh, A., Ahmad, A., Al-Joudi, A. S., Al-Gahtani, H. B., & Al-Qahtani, M. S., (2014). Social networks' benefits, privacy, and identity theft: KSA case study. *International Journal of Advanced Computer Science and Applications, 5*(12), 129-143. doi:10.14569/ijacsa.2014.051218

Demarest, J. M. (2014). Statement before the Senate Committee on Banking, Housing, and Urban Affairs. Retrieved fromhttps://www.banking.senate.gov/public/_cache/files/4e192807-e9f9-4c53-9283-ea4e4198aee0/23C6AE00CC53D93492511CC744028B5E.demaresttestimony121014.pdf

De Massis, A., & Kotlar, J. (2014). The case study method in family business research: Guidelines for qualitative scholarship. *Journal of Family Business Strategy*, *5*(1), 15-29. doi:10.1016/j.jfbs.2014.01.007

Demshock, H. M. (2016). What can be done to combat tax-related identity theft? *Journal of Financial Service Professionals*, *70*(3), 16-19. Retrieved from http://www.financialpro.org/pubs/journal_index.cfm

Dube, J. F. (2011). Fraud in health care and organized crime. *Medicine & Health Rhode Island*, *94*(9), 268-269. Retrieved from http://www.rimed.org/medhealthri/2011-09/2011-09-268.pdf

Dyer, O. (2015). US healthcare kickback schemes come under heavy scrutiny. *BMJ*, *350*(1), 1230-1230. doi:10.1136/bmj.h1230

Edwards-Jones, A. (2014). Qualitative data analysis with NVIVO. *Journal of Education for Teaching*, *40*(2), 193–195. doi:10.1080/02607476.2013.866724

Eide, E. R., & Showalter, M. H. (2012). Methods matter: Improving causal inference in educational and social science research: A review article. *Economics of Education Review*, *31*, 744-748. doi:10.1016/j.econedurev.2012.05.010

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. *Sage Open*, *4*(1), 1-10. doi:10.1177/2158244014522633

Enthoven, A. C. (2014). *Theory and practice of managed competition in health care finance*. New York, NY: Elsevier.

False Claims Act. California Government. Code §§ 12650-12656. Retrieved from http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov &group=12001-13000&file=12650-12656

Farooq, M. B. (2015). Qualitative telephone interviews: Strategies for success. *Qualitative Research, 12*(6), 1-30. doi:10.1177/1468794112439005

Federal Trade Commission. (2014). Identity-theft complaints in 2014. Washington, DC: Author. Retrieved from https://www.google.com/search?q= child+i.d+thefts

Federal Trade Commission. (2016). *Consumer sentinel network data book for January December 2015*. Washington, DC: Federal Trade Commission. Retrieved from http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2015.pdf

Ferrillo, P., & Singer R. (2015). Is employee awareness and training the holy grail of cybersecurity? *The Corporate Governance Advisor, 23*(3), 1-28. Retrieved from http://www.agg.com/files/uploads/5-15%20(3).pdf

Fiske, S. T., & Hauser, R. M. (2014). Protecting human research participants in the age of big data. *Proceedings of the National Academy of Sciences*, *111*(38), 13675-13676. doi:10.1073/pnas.1414626111

Francis, J. J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M. P., & Grimshaw, J. M. (2010). What is an adequate sample size? Operationalizing data saturation for theory-based interview studies. *Psychology and Health*, *25*(10), 1229–1245. doi:10.1080/08870440903194015

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling & Development, 91*(2), 184–194. doi:10.1002/j.1556-6676.2013.00085.x

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*(9), 1408-1416. doi:10.1080/08941920.2014.888791

Gaskin, D. (2012). Recent developments in health law. *Journal of Law, Medicine, & Ethics, 40,* 160-175. doi:10.1111/j.1748-720X.2012.00655.x

Goering, P. N., & Streiner, D. L. (2013). 19 reconcilable differences: The marriage of qualitative and quantitative methods. In A. Author & B. Author, *A guide for the statistically perplexed: Selected readings for clinical researchers* (pp. 225-239). Toronto, Canada: University of Toronto Press.

Goertz, G., & Mahoney, J. (2012). A tale of two cultures: Qualitative and quantitative research in the social sciences. *International Journal of Market Research, 57*(6), 959-961. doi:10.1515/9781400845446.

Gottschalk, P., & Solli-Sather, H. (2011). Influence of white-collar crime on corporate reputation: An opinion survey of chief financial officers. *International Journal of Corporate Governance, 2*, 95-105. doi:10.1504/IJCG.2011.041149

Guo, K., Smith, C., Powell, K., & Nicholls, K. (2012). Consistent left gaze bias in processing different facial cues. *Psychological Research, 76,* 263-269. doi:10.1007/s00426-011-0340-9

Harrell, E. (2015). Victims of identity theft, 2014. *Bureau of Justice Statistics*, *248991*(1), 1-26. Retrieved from http://www.bjs.gov/content/pub/pdf/vit14.pdf

Hedayati, A. (2012). An analysis of identity theft: Motives, related frauds, techniques and prevention. *Journal of Law and Conflict Resolution*, *4*(1), 1-12. doi:10.5897/JLCR11.044

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Information Management & Computer Security*, *21*(4), 266-287. doi:10.1108/imcs-08-2012-0043

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime*, *22*(2), 242-260. doi:10.1108/jfc-09-2013-0055

Huang, X., & Du, X. (2015). Achieving data privacy on hybrid cloud. *Security and Communication Networks, 8*(18), 3771–3781. doi:10.1002/sec.1298

Hunter, D. (2003). Cyberspace as place and the tragedy of the digital anti-commons. *California Law Review*, 91(2), 439. doi:10.2307/3481336

Hussein, A. (2015). The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined? *Journal of Comparative Social Work*, *4*(1). Retrieved from http://journal.uia.no/index.php/JCSW/article/viewFile/212/147

Jaeger, J. (2013). Enforcement & litigation: Report shows healthcare fraud enforcement targets. *Compliance Week, 10*(116), 3. Retrieved from https://www.complianceweek.com/

Januleviciute, J., Askildsen, J. E., Kaarboe, O., Siciliani, L., & Sutton, M. (2015). How do Hospitals Respond to Price Changes? Evidence from Norway. *Health Economics*, *25*(5), 620–636. doi:10.1002/hec.3179

Johnson, J. S. (2014). Qualitative sales research: An exposition of grounded theory. *Journal of Personal Selling & Sales Management*, *35*(3), 262–273. doi:10.1080/08853134.2014.954581

Johnson, M., Baxter, S., Blank, L., Cantrell, A., Brumfitt, S., Enderby, P., & Goyder, E. (2015). The state of the art in non-pharmacological interventions for developmental stuttering. Part 2: qualitative evidence synthesis of views and experiences. *International Journal of Language & Communication Disorders*, *51*(1), 3–17. doi:10.1111/1460-6984.12182

Jürges, H., & Köberlein, J. (2015). What explains DRG upcoding in neonatology? The roles of financial incentives and infant health. *Journal of Health Economics, 43*, 13-26. doi:10.1016/j.jhealeco.2015.06.001

Kaufman, B. G., Thomas, S. R., Randolph, R. K., Perry, J. R., Thompson, K. W., Holmes, G. M., & Pink, G. H. (2016). The rising rate of rural hospital closures. *The Journal of Rural Health*, *32*(1), 35-43. doi:10.111/jh.12128

Keehan, S. P., Poisal, J. A., Cuckler, G. A., Sisko, A. M., Smith, S. D., Madison, A. J., Lizonitz, J. M. (2016). National Health Expenditure Projections, 2015-25: Economy, prices, and aging expected to shape spending and enrollment. *Health Affairs*, 35(8), 1522–1531. doi:10.1377/hlthaff.2016.0459

Khey, D. N., & Sainato, V. A. (2013). Examining the correlates and spatial distribution of organizational data breaches in the United States. *Security Journal, 26,* 367-382. doi:10.1057/sj.2013.24

Kieke, R. L. (2014). Recent privacy breach settlements illustrate the importance of proactively pursuing compliance. *Journal of Health Care Compliance, 27*(12), 41-52. Retrieved from http://www.aspenpublishers.com

Krstić, M. (2014). Rational choice theory and addiction behavior. *Faculty of Economics and Business*, *26*(2), 163-177. Retrieved from http://www.efzg.hr/trziste

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. *Computers & Security*, *45*(1), 58–74. doi:10.1016/j.cose.2014.05.006

Lawrence, J., & Tar, U. (2013). The use of grounded theory technique as a practical tool for qualitative data collection and analysis. *Electronic Journal of Business Research Methods*, *11*, 29-40. Retrieved from http://www.ejbrm.com/main.html

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design* (11th ed.). New York, NY: Pearson

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G & Wolff, S. S. (1997). The past and future history of the Internet. *Communications of the Association of Computing Machinery,* 40(2), 102-108. doi:10.1145/25371.253741

Lo, C. O. (2014). Enhancing groundedness in realist grounded theory research. *Qualitative Psychology, 1*(1), 61–76. doi:10.1037/qup0000001

Loh, E. (2012). How and why doctors transition from clinical practice to senior hospital management: A case research study from Victoria, Australia. *The International Journal of Clinical Leadership*, *17*(4), 235-244. Retrieved from http://www.radcliffe-oxford.com

Li, T., & Slee, T. (2014). The effects of information privacy concerns on digitizing personal health records. *Journal of the Association for Information Science and Technology*, *65*(8), 1541–1554. doi:10.1002/asi.23068

Luizzo, A., & Scaglione, B. (2014). Aspects of controlling fraud in healthcare facilities: taking the threat seriously. *Journal of Healthcare Protection Management*, *28*(1), 21-27. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/22423517

Mackey, T. K., & Liang, B. A. (2012). Combating healthcare corruption and fraud with improved global health governance. *BMC International Health and Human Rights, 12*(1). doi:10.1186/1472-698x-12-23

Madensen, T. D. (2009). Environmental criminology and crime analysis. *International Criminal Justice Review*, *19*(2), 225-226. doi:10.1177/1057567709332526

Madsen, A. K. (2013). Virtual acts of balance: Virtual technologies of knowledge management as co-produced by social intentions and technical limitations. *Electronic Journal of E-Government, 11*(2), 183-197. Retrieved from http://www.ejeg.com/main.html

Mancini, M. (2014). Medical identity theft in the emergency department: Awareness is crucial. *Western Journal Emergency Medicine*: *Integrating Emergency Care with Population Health, 15*, 899-901. doi:10.5811/westjem.2014.8.22438

Mann, L. (2013). How to reduce the risk of purchasing fraud. *Healthcare Financial Management, 67*(7), 78-82. Retrieved from http://www.hfma.org/

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58. doi:10.1509/jm.15.0497

Matthews, R. (2014). Rational choice, routine activities and situational crime prevention. *Realist Criminology*, 72–93. doi:10.1057/9781137445711_4

McManus, J., & Mosca, J. (2015). Strategies to build trust and improve employee engagement. .*International Journal of Management & Information Systems*, *19*(1), 37-42. doi:10.19030/ijmis.v19i1.9056

McNabb, J., & Rhodes, H. B. (2014). Combatting the privacy crime that can kill. *American Health Information Management Association, 85*(4), 26-29. Retrieved from http://library.ahima.org/doc?oid=300413#.WKyrAP4zVp8

Melnik, T. (2014). Doctors, unhappy with their EHR system, sue the vendor in a class action, 16(1), 51-54. Retrieved from http://melniklegal.com/av/2014_01_ JHCC_Allscripts_EHR_Class_Action.pdf

Metcalf, J. (2016). Big data analytics and revision of the common rule. *Communications of the ACM*, *59*(7), 31-33. doi:10.1145/2935882

Miller T. R, Wiek, A., Sarewitz, D., Robinson, J., Olsson, L., Kriebel, D., & Loorbach, D. (2013). The future of sustainability science: a solutions-oriented research agenda. *Sustainability Science*. doi:10.1007/s11625-013-0224-6

Miner-Romanoff, K. (2012). Interpretive and critical phenomenological crime studies: A model design. *Qualitative report, 17*(54), 1-32. Retrieved from http://www.nova.edu/ssss/QR/QR17/miner-romanoff.pdf

Mohammed, D., & Mariani, R. (2014). An evaluation of the cybersecurity policies for the United States health & human services department: Criteria, regulations, and improvements. *International Journal of Research in Business and Social Science, 4*(4), 1-7. Retrieved from http://www.saintleo.edu/media/975948/an_ evaluation_of_the_cybersecurity_policies.pdf

Mohan, A. (2014, Month). A medical domain collaborative anomaly detection framework for identifying medical identity theft. 2014 International Conference on Collaboration Technologies and Systems (CTS). doi:10.1109/cts.2014.6867600

Moore, J. W. (2010). From phishing to advanced persistent threats: The application of cybercrime risk to the enterprise risk management model. *Review of Business Information Systems, 14*(4). Retrieved from http://www.aspenpublishers.com

Moses, R., & Jones, D. S. (2014). Physician assistants in health care fraud: Vicarious liability. *Journal of Health Care Compliance, 13*(2), 51-75. Retrieved from http://www.aspenpublishers.com

Moustakas, C. E. (1994). *Phenomenological research methods*. Thousand Oaks, CA: Sage Publications.

Mulig, E., Smith, L. M., & Stambaugh, T. (2015). Identity hack! Is your company next? *Strategic Finance, 96* (12), 33-39. Retrieved from https://ssrn.com/abstract=2614554

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2013). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health Services Research, 40,* 1-12. doi:10.1007/s10488-013-0528-y

Patel, K., & Sherer, J. D. (2016). DOJ targets individuals for violations of False Claims Act and Anti-Kickback Statute. *Journal of Health Care Compliance*, *18*(4), 53-56. Retrieved from http://www.aspenpublishers.com

Policastro, C., & Payne, B. (2015). Can you hear me now? Telemarketing fraud victimization and lifestyles. *American Journal of Criminal Justice, 40,* 620-638. doi:10.1007/s12103-014-9279-x

Pozzebon, M., Rodriguez, C., & Petrini, M. (2014). Dialogical principles for qualitative inquiry: A nonfoundational path. *International Journal of Qualitative Methods*, *13*(1), 293–317. doi:10.1177/160940691401300114

Price, M., & Norris, D. M. (2009). Health care fraud: Physicians as white collar criminals? *Journal of the American Academy of Psychiatry and Law*, *37*(3), 286-289. Retrieved from http://www.jaapl.org/

Premalatha, P. (2016). Role of manager-employee relationships in retaining knowledge workers in IT industry. *The Indian Journal of Industrial Relations*, *51*(3), 418-432

Przyswa, E. (2013). Counterfeit medicines and criminal organizations. International Institute of Research against Counterfeit Medicines, 129. Retrieved from https://hal-mines-paristech.archives-ouvertes.fr/hal-00958233

Rao, U. H., & Nayak, U. (2014). Malicious Software and Anti-Virus Software. The InfoSec Handbook, 141–161. doi:10.1007/978-1-4302-6383-8_7

Reader, G. G., Jesilow, P., Pontell, H. N., & Geis, G. (1995). Prescription for Profit: How Doctors Defraud Medicaid. Journal of Public Health Policy, *16*(2), 250. doi:10.2307/3342600

Reeler, D. (2015). Exploring the real work of social change. *Organizational Studies Practitioner*, 47(1), 15-24. Retrieved from http://www.aspenpublishers.com.

Reeler, D. (2016). Exploring the real work of social change: Seven questions that keep us awake. Leading and managing in the social sector, 57-74. doi:10.1007/978-3-319-47045-0_5.

Reeves, S., Peller, J., Goldman, J., & Kitto, S. (2013). Ethnography in qualitative educational research: AMEE Guide No. 80, Medical Teacher. *US National Library of Medicine National Institutes of Health*, *35*, e1365-e1379. doi:10.3109/0142159X.2013.804977

Roberts, S. J. (2014). The necessity of information security in the vulnerable pharmaceutical industry. *Journal of Information Security*, *5*(4), 147-153. doi:10.4236/jis.2014.54014

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2) 121-135. doi:10.1093/cybsec/tyw001

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, *11*, 74-104. doi:10.1111/jels.12035

Ruankaw, T. (2016). Fraud Theories (Triangle, Diamond, M.I.C.E., Scale, Pentagon, and Gone). Retrieved from http://lintangmaharaniiii.blogspot.com/2017/04/fraud-theories-triangle-diamond-mice.html

Rubin, H. J., & Rubin, I. S. (2012). *Qualitative interviewing: The art of hearing data* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.

Ruggeri, K., Záliš, L., Meurice, C. R., Hilton, I., Ly, T.-L., Zupan, Z., & Hinrichs, S. (2015). Evidence on global medical travel. *Bulletin of the World Health Organization, 93*(11), 785-789. doi:10.2471/blt.14.146027

Rutkin, A., & Tugander, R. (2015). Coverage question concerning cybercrimes. *FDCC Quarterly, 64*(2), 114. Retrieved from http://www.thefederation.org

Sack, K. (2012, October 8). Researchers wring hands as U.S. clamps down on death record access. *The New York Times*, 1-4. Retrieved from http://www.nytimes.com/2012/10/09/us/social-security-death-record-limits-hinderresearchers.html?hp&_r=0

Satter, M. Y. (2014). Critical care: The far-reaching effects of medical identity theft. *Medical Identity Fraud Alliance*, *34*(6), 1-5. Retrieved from http://medidfraud.org/critical-care-the-far-reaching-effects-of-medical-identity-theft/

Scanio, S., & Ludwig, R. W. (2013). Surging swift and liable? Cybercrime and electronic payments fraud involving commercial bank accounts. Who bears the loss? *Journal of Internet Law*. Retrieved from http://ejil.oxfordjournals.org

Scholl, S. G., Greifeneder, R., & Bless, H. (2013). When fluency signals truth: Prior successful reliance on fluency moderates the impact of fluency on truth judgments. *Journal of Behavioral Decision Making*, *27*(3), 268–280. doi:10.1002/bdm.1805

Schweitzer, J. (2012). Reconciliation of the cloud computing model with US federal electronic health record regulations. *Journal of the American Medical Informatics Association, 19*(2), 161-165. doi.org/10.1136/amiajnl-2011-000162

Selamat, M. H., & Babatunde, D. A. (2014). Mediating effect of information security culture on the relationship between information security activities and organizational performance in the Nigerian banking setting. *International Journal of Business and Management*, *9*(7), 33-38. doi:10.5539/ijbm.v9n7p33

Sen, R., & Borle, S. (2015). Estimating the context risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314–341. doi:10.1080/07421222.2015.1063315

Serban, A., & Roberts, A. J. B. (2016). Exploring antecedents and outcomes of shared leadership in a creative context: A mixed-methods approach. *The Leadership Quarterly*, *27*(2), 181–199. doi:10.1016/j.leaqua.2016.01.009

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, *55*(4), 249-356. doi:10.1016/j.bush0r.2012.02.004

Sharma, A., & Baweja, P. (2017). Medical identity theft: A case report. *Annals of Internal Medicine*, *166*(5), 380. doi:10.7326/l16-0360

Sims, J. M. (2010). A brief review of the Belmont Report. *Dimensions of Critical Care Nursing*, *29*(4), 173–174. doi:10.1097/dcc.0b013e3181de9ec5

Social Security Act § 1128B(b). Retrieved from http://www.ssa.gov/OP_Home/ssact/title11/1128B.htm

Stallings, S. S., & Caravello, L. E. (2013). Wait not, want not: The importance of the statute of limitations in Qui Tam False Claims Act cases. *Pittsburgh Journal of Environmental and Public Health Law*, *7*(2). doi:10.5195/pjephl.2013.50

Statista (2015). Number of worldwide internet users from 2000 to 2014 (in millions). Retrieved from http://www.statista.com/statistics/273018/number-of-internet-users-worldwide

Straus, S. E., Johnson, M. O., Marquez, C., & Feldman, M. D. (2013). Characteristics of successful and failed mentoring relationships: a qualitative study across two academic health centers. *Academic Medicine: Journal of the Association of American Medical Colleges*, *88*(1), 82. doi:10.1097/ACM.0b013e31827647a0

Sun, T., & Wang, X. (2013). Research of data security model in cloud computing platform for SMEs. *International Journal of Security and Its Applications*, 7(6), 97-108. doi:10.14257/ijsia.2013.7.6.10

Taitsman, J. K., Grimm, C. M., & Agrawal, S. (2013). Protecting patient privacy and data security. *The New England Journal of Medicine*, *368*, 977-979. doi:10.1056/NEjMp1215258

Tajpour, A., Ibrahim, S., & Zamani, M. (2013). Identity theft methods and fraud types. *IJIPM: International Journal of Information Processing and Management, 4*(7), 51-58. Retrieved from https://www.researchgate.net/publication/273259976

Taylor, S. J., Bogdan, R., & DeVault, M. (2015). *Introduction to qualitative research methods: A guidebook and resource*. Hoboken, NJ: John Wiley & Sons.

Terry, N. P. (2014). Big data proxies and health privacy exceptionalism. *Journal of Law-Medicine, 24*(1), 65-108. doi:10.2139/ssrn.2320088

Thornton, D., Brinkhuis, M., Amrit, C., & Aly, R. (2015). Categorizing and describing the types of fraud in healthcare. *Procedia Computer Science, 64*, 713–720. doi:10.1016/j.procs.2015.08.594

U.S. Department of Health and Human Services. (2016). *HIPAA for individuals*. Retrieved from http://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/

U.S. Department of Justice. (2016). National health care fraud takedown results n charges against 301 individuals for approximately $900 million in false billing. Retrieved from https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-charges-against-301-individuals-approximately-900

U.S. Government Accounting Office. (2013). *GAO's 2013 high-risk update Medicare and Medicaid* (GAO Publication No. GAO-13-433T). Retrieved from http://gao.gov/assets/660/652386.pdf

U.S. Government Accountability Office. (2016a). Health care fraud: Information on most common schemes and the likely effect of smart cards. GAO Publication No. GAO-16-216). Retrieved from http://www.gao.gov/assets/680/674771.pdf

U.S. Government Accountability Office. (2016b). *Medicare advantage: Fundamental improvements needed in CMS's effort to recover substantial amounts of improper payments*. Retrieved from http://www.gao.gov/assets/680/676441.pdf

Van Biljon, J. (2014). Questioning the questionnaire: Expediency of reviewing and publication versus adequate description and methodological justification. *8th European Conference on IS Management and Evaluation*, 262-270. Retrieved from http://hdl.handle.net/10500/18377

Venkatesh, V., & Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *Management Information Systems Quarterly*, *37*, 21-54. Retrieved from http://www.misq.org

Vittadini, G., Berta, P., Martini, G., & Callea. (2012). The effect of a law limiting upcoding on hospital admissions: Evidence from Italy. *Empirical Economics*, *42*(2), 563-582. doi:10.1007/s00181-012-0548-6.

Votta, N. (2016). Medical identity theft: Part 1 (Briefing on HIPAA), *Medical Identity Fraud Alliance*, 241-244. Retrieved from http://medidfraud.org/medical-identity-theft-part-1-briefings-on-hipaa/

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *Management*

Information Systems Quarterly, *39*(1), 91-112. Retrieved from http://misq.org/misq/downloads

Ward, K., Gott, M., & Hoare, K. (2015). Participants' views of telephone interviews within a grounded theory study. *Journal of Advanced Nursing, 71*(12), 2775–2785. doi:10.1111/jan.12748

Wells, A. (2013). The importance of design thinking for technological literacy: A phenomenological perspective. *International Journal of Technology & Design Education*, *23*, 623-636. doi:10.1007/s10798-012-9207-7

Wittmayer, J. M., & Schäpke, N. (2014). Action, research and participation: roles of researchers in sustainability transitions. *Sustainability Science*, *9*(4), 483–496. doi:10.1007/s11625-014-0258-4

Xu, Z. (2012). Victimized by phishing: A heuristic-systematic perspective. *Journal of Internet Banking and Commerce*. Retrieved from www.zcxu@fudan.edu.cn

Yao, J. (2017). Analysis of Management Fraud in listed companies based on Fraud Triangle Theory. *DEStech Transactions on Social Science, Education and Human Science*, (aetms). doi:10.12783/dtssehs/aetms2017/15857

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education, 48*(2), 311–325. doi:10.1111/ejed.12014

Yin, R. K. (2012) *Qualitative research from start to finish.* Thousand Oaks, CA: Sage Publications

Yin, R. K. (2013). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage.

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage Publication, Inc.

Zivkovic, J. (2012). Strengths and weaknesses of business research methodologies: Two disparate case studies. *Business Studies Journal*, *4*(2), 91-99. Retrieved from http://alliedacademies.org/Public/Default.aspx

Appendix A: Interview Questions

Participant #: ____

Interview Questions

1. What strategies do you use to reduce IT and MIF to improve business performance?
2. What hurdles did you face in developing and implementing strategies to improve business performance and how did you address the barriers?
3. How do you revise the strategies to address changing conditions?
4. What processes are in place to protect electronic records?
5. What processes are in place to protect paper records?
6. How would you stop an imposter from using other patients' identities?
7. What else you would like to add that we have not discussed about IT and MIF?

Appendix B: Informed Consent

Consent Form

Dear Potential Participant,

You are invited to participate in a research study in determining the strategies medical business leaders use to prevent and reduce medical identity fraud to increase business performance in the state of New York. The researcher is inviting small medical practice owners and/or partial owners with the knowledge to participate in this study. Owners/partial owners of a medical business with 25 or fewer employees must be in business for at least 5 years with experience working in the healthcare arena and/or experience working at the Social Security Office.

This form is part of a process called *informed consent* to enable you to understand this study before deciding whether or not to participate. This study is being conducted by Junior V. Clement who is a doctoral student at Walden University. Research from this study will be used to explore the successful strategies some Healthcare Leaders (HL) used in the state of New York to reduce identity theft (IT) and medical identity fraud (MIF) to improve business performance.

Background Information:

The purpose of this study is to explore the strategies some HLs use to reduce IT and MIF to improve business performance. The target population will comprise of HLs in the state of New York. MIF places a major burden on patient care due to substantial revenue losses as eradicating or reducing the crisis could affect positive social change by

improving healthcare delivery, patient care, and attenuate the increasing cost of medical care for more members of society.

Procedures:

If you agree to be in this study, you will be asked to:

● Participate in a telephone interview for approximately 20 to 30 minutes.

● During the session of this study, digital recording was conducted for the duration of the telephone interview for a maximum of 30 minutes.

● For further clarification, you might be asked to participate in a brief 20 minutes follow-up session to get more details within 1 week after the original interview, if necessary.

● A copy of the transcript was sent to review for accuracy and updating if necessary. Please review the transcript within 30 minutes and return to me via email upon completion.

Voluntary nature of the study:

This study was voluntary. Everyone will respect your decision of whether or not you choose to be in the study. No representative will treat you differently if you decide not to be in the study. If you decide to join the study now, you can still change your mind later as you reserve the right to stop at any time. You reserve the right to stop the interview at any time without notice.

Risk and benefits of being in the study:

There was no foreseeable risk or harm regarding your safety. The author of this report hopes the perspectives captured from telephone interviews during the study lead to innovative solutions to share as a benefit to others HLs and leaders in other industries.

Payment:

There was no payment, gifts, or reimbursements granted in exchange for your participation in this study but respondents' participation was greatly appreciated!

Privacy:

Any information you provide will be kept confidential as actual names are omitted from the study. The researcher will not use your personal information for any purposes outside of this research project. Also, the researcher did not include your name or anything personal details that could identify you in the study reports. Data will be kept secured by Junior Clement in a locked fire proof safe located in my residence in the state of New York. Recorded data will be permanently stored in a fire proof safe for a period of 5 years as required by Walden University. After 5 year expires, hard copy information will be destroyed in a crossed-cut shedder and discarded to prevent the information from falling into thieves' hands.

Contact and questions:

Please feel free to ask any questions you have now. Or, if you have questions later, you may contact the researcher via person cell phone at 917-748-2825 or electronic mail (email) address at: Junior_20747@hotmail.com. If you want to talk privately about your rights as a participant, you may call the university Research Participant Advocate at 800-925-3368 ext. 3121210 or email address: irb@mail.waldenu.edu. Walden University's approval number for this study is 10-11-17-0533495 and it expires on October 10th, 2018.

Acquiring the Statement of Consent:

If you are interested in participating in this study, please indicate your consent by replying with the words “I Consent”. Please retain a copy of this consent form for your records.

Appendix C: Interview Protocol Form

Interview Title: Strategies to Prevent and Reduce Medical Identity Theft Resulting in Medical Fraud.

1. Each telephone interview started with an introduction or greeting.
2. I thanked participants for taking time to participate in this study.
3. I send the consent form to participants prior to the interview and ask each person to retain a copy of the form if he or she decided to participate in the study.
4. I alerted participants that the recording session will start for the interview.
5. I turned on the recording device after getting the thumbs from participants.
6. Interview session started with question one and persist until the last question.
7. From start to end, participants had the liberty to speak freely on the topic.
8. At the end of the interview, participants were alerted about member checking to ensure reliability and validity of the information captured during interviews.
9. After interpreting the transcript, I contacted each participant and schedule 20 to 30 minute sessions for member checking sessions to ensure reliability and validity from the data participants' shared during the interviews.
10. I ensured participants had my contact number to answer their questions.
11. To end the interview, I thanked participants for participating in this study.