Medical Information Security

William C. Figg, Ph.D. *William.figg@dsu.edu*
Dakota State University Business and Information Systems Madison, SD 57042 USA

Hwee Joo Kam, M.S. *hkam@nemich.edu*
North Central Michigan College Computer Information Systems Petoskey, MI 49770 USA

Abstract

Modern medicine is facing a complex environment, not from medical technology but rather government regulations and information vulnerability. HIPPA is the government's attempt to protect patient's information yet this only addresses traditional record handling. The main threat is from the evolving security issues. Many medical offices and facilities have multiple areas of information security concerns. Physical security is often weak, office personnel are not always aware of security needs and application security and transmission protocols are not consistently maintained.

Health insurance needs and general financial opportunity has created an emerging market in medical identity theft. Medical offices have the perfect storm of information collection, personal, credit, banking, health, and insurance. Thieves have realized that medical facilities have as much economic value as banks and the security is much easier to crack. Mostly committed by insiders, medical identity theft is a well-hidden information crime. In spite of its covert nature, the catastrophic ramification to the victims is overt. This information crime involves stealing patients' records to impersonate the patients in an effort of obtaining health care services or claiming Medicare on the patients' behalf. Unlike financial identity theft, there is a lack of recourse for the victims to recover from damages. Medical identity theft undermines the quality of health care information systems and enervates the information security of electronic patient record.

Keywords: Medical Identity Theft, Electronic Patient Record, Information Crime, Information Security

1. INTRODUCTION

Medical offices have in the past focused on the gathering and disseminating information for the efficient treatment of patient maladies. Security was often limited to traditional methods of locking file rooms or file cabinets. The introduction of computers increased the efficiency of medical record keeping but it also increased the security exposure. Computer management of records took information from the hands of a manageable few and created opportunities for leaks, mismanagement and outright theft.

Why would anyone be interested in medical information? If the medical facility's gathering of information is considered the value is easily understood. Records contain personal information including the big three; birthday, social security numberand address. The second portion is financial with the repeat of the previous plus credit and banking information. The last focus is the medical information with the possibility of embarrassment or even blackmail.

The advent of electronic patient records has inadvertently created opportunities to health care frauds including medical identity theft. Inaccurate medical records may lead to medical mistreatment that will cause catastrophic consequences to a patient. Literature reviews show the paucity of this research topic. Not many literatures discuss about the crime of medical identity theft and the ramification of data security

breaches in health care. Perpetrators treat victims merely as a commodity and they show a complete lack of concern for the damages they did to patients' health and to the health care systems [31]. Many assume that medical identity theft is no different from financial identity theft but in fact medical identity theft has more devastating effects on patients for there is a lack of recourse for patient to correct the false entries in their medical records. In reality, false medical information can kill a patient.

2. ELECTRONIC PATIENT RECORD

In health care industry, patients' data are vastly shifting from paper records to electronic records. Electronic patient record is a computer based memory that can be assessed over networks both internally and externally and it is highly structured, ordered and classified by a unique identifier [27]. Specifically, electronic patient record contains all the health care related information of a patient and combines several enterprise-based electronic medical records concerning one patient [30]. Electronic patient records changed the way patients' information is stored. The adoption of electronic patient records is growing [12]. Moving towards electronic based health care systems enables health providers streamline automated processes as well as specific applications that can help doctors with diagnosis and treatment of patients [14]. In addition, the implementation of electronic patient records serves the purposes of electronic billing, telemedicine, and worldwide data mining of health trend [17].

Electronic patient records, however, are a double-edged sword. With the advent of electronic patient records, patients' data can easily be shared among physicians, health care providers, nurses, supporting staff, medical research, and public health care services [30]. Basically, most health care information including patients' data is not generated solely within a physician/patient relationship, but is generated from the diverse sources, such as non-physician specialist, nurse practitioners, public health officers, laboratories, and other ancillary health care professions [16]. The sharing as well as distribution of patient information enables productive medical research, proper treatment of patients, and improvement in health care quality. On the other hand, electronic patient records pose a challenge to maintain information confidentiality, integrity, and availability – (1) the computerized record infers that the requester has the same hardware and software communication protocol and thus enables easy access to data [27]. This may open doors to the unauthorized parties who may unscrupulously steal patients' data for personal benefits, alter patients' records, and expose patients' medical history. In other words, the high accessibility of patients' data has made it easier for perpetrators to invade patients' information confidentiality, integrity, and availability and commit health care fraud. Many healthcare experts are worried that as industry moves toward the adoption of electronic patient records, the threat of medical identity theft poses a growing challenge and places patients at a greater risk [29]. Similarly, the proposed National HealthcareInformation Network (NHIN) mandated by President Bush's 2004 Executive Order may increase the risk of patients' information security. (2) Another problem is the operational issue in health care setting: the electronic patient records are not kept in one designated location due to the interoperability of the Integrated Delivery Systems (IDS). The records can be viewed by the government agencies, regional health database organizations or information brokers under the Integrated Delivery Systems (IDS). The unauthorized parties who work in the health care setting may have the opportunities to call up a screen to view the patient-based data. (3) Inventive persons might circumvent obstacles to access data by borrowing passwords or smart cards and then transmit the data world-wide over networks or compare sensitive data from various resources [27]. Given that, the implementation of electronic patient records that is initially meant to streamlining automated health care processes and improving health care quality have unintentionally encouraged patients' data security breaches and health care fraud.

3. TECHNOLOGY AS A SECURITY MECHANISM

Technology advancement that has led to the implementation of electronic patient record is not really the culprit of patients' privacy and security breaches. Amid the threats of health care fraud and violation of patients' information security, there are security mechanisms available to safeguard electronic patient records. The following studies exemplify the application of information technology that serves the purpose of protecting patients' information security. (1) The distributed information architecture for public health adopts a distributed data storage approach to protect patients' information. A distributed database is deployed to prevent the creation of a monolithic repository, vulnerable to breach or misuse [24]. (2) A

research conducted by University of Michigan imposes security mechanism to protect sensitive health data. A system called the "honest broker" is developed to embark upon the issue of health information security. The Honest Broker (HB) is built on the two-component architecture – the non-identifiable data is stored in a separate system whereas the identifiable data is stored in another system. HB meditates between these systems and manages data transfer and electronic storage of personal health identifiers [4]. This architecture increases the burden on attackers who need to compromise two systems in order to match the identifiable record with the non-identifiable one. (3) Technology can mitigate the threat of the de-identification of anonymous data and reduce the risks involving the linkability of genomic data such as DNA. A patient's location visit pattern, or "trail", can be constructed because patients are mobile and their data can be collected and shared by multiple health care organizations. The uniqueness of patient's trail can link to a patient's record, revealing a patient's identity. A formal privacy protection model called k-unlinkability is introduced to thwart the trail re-identification and prevent the tracing of DNA records of a patient [22]. This model adopts computational basis and is configured to strip off patients' identifiers in a biomedical database.

4. HEALTH CARE MANAGEMENT AND ADMINISTRATION

Although the aforementioned security mechanism supported by information technology can assuage the violation of patients' information security, a few literatures have unveiled the fact that non technical challenges such as administrative and management issue have adversely impacted patients' information security and posed a thorny issue. Currently, the health care industry lacks precise instrumentation and makes no serious attempt to measure health care fraud; there has been attempt initiated by Office of Inspector General (OIG) to institute its annual audit program but the weak methodology produces only low loss estimates [31]. Furthermore, health care administration and management have permitted patients' information to be reviewed and used without patients' consent in the name of cost saving, quality improvement, public health, advances in research, and other commendable goals [1]. For instance, insurance companies, managed health care organizations, and health care employees are interested to access individual's medical records in an attempt to reduce expenses [17]; managed care companies insist on reviewing medical charts to determine if care should be authorized; accrediting bodies want to ensure that the clinicians' notes are detailed and complete; government agencies seek identifiable information for planning purposes; and law enforcement agencies see medical records a mean to identify and convict wrongdoers [1].

5. DATA SECURITY BREACHES: MEDICAL IDENTITY THEFT

Given that many parties can view patients' medical records without patients' knowledge, data security breaches in health care have unfortunately become common. According to William Wikenwerder, the assistant secretary of defense for health affairs, privacy and security are the Chernobyl that is waiting to happen for the healthcare industry [5]. Among the data security breaches in health care, the newly emerging health care privacy threat is medical identity theft, which is considered a crime. Byron Hollis, director of the antifraud department at the Blue Cross and Blue Shield Association, mentioned that "medical identity theft is the fastest-growing form of health care fraud" (Pear, 2008). Through 2005, there have been nearly 18,000 cases of medical identity theft or about 1.8% of all identity theft cases reported to Federal Trade Commission (FTC) [5]. According to World Privacy Forum, there have been 19, 428 complaints regarding medical identity theft to the Federal Trade Commission (FTC) since 1992, the earliest date the FTC started to process the complaints; and the number of people who experienced medical identity theft rose from 1.6 percent in 2001 to 1.8 percent in 2005 [9]. In addition, the World Privacy Forum issued a report revealing that the growing of medical phenomenon is estimated to have impacted as many as 3.25 million people [3].

6. WHAT IS MEDICAL IDENTITY THEFT?

Identity theft, essentially, refers to the appropriation of an individual's personal information in order to impersonate that person for one's financial gain or other benefits [32]. In this regard, medical identity theft is defined as an occurrence in which a person uses another person's identity such as person's name, insurance information, Medicaid number or social security number, without the person's knowledge and consent, to obtain medical care or services or to generate a plethora of bogus medical bills for the purpose of claiming Medicare[8]. According to World Privacy Forum, medical identity theft is an

information crime and a health crime that can have medical, financial and other impacts [9]. The victims of medical identity theft can be patients, physicians, and nurses. Strictly speaking, medical identity theft is part of health care fraud, which, according to National Health Care Anti-Fraud Association, is *an intentional deception or misrepresentation that the individual or entity makes knowing that the misrepresentation could result in some unauthorized benefit to the individual, or the entity or to some other party*[25]. In the context of law, health care fraud is defined as whoever knowingly and willfully executes, or attempts to execute, a scheme or artifice - (1) to defraud any health care benefit program; or (2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program (Legal Information Institution, Cornell University Law School). Although medical identity theft can fit into the legal definition above, it is best understood in the context of information crime - a very sophisticated crime that involves theft or abuse of identity information and causes financial losses to victims, health care provides, and insurers.

7. MEDICAL IDENTITY THEFT VS. FINANCIAL IDENTITY THEFT

Medical identity theft is under-report, under-research and poorly documented [13]. Many people assume that medical identity theft is no different from financial identity theft but there are differences among these two: (1) Financial identity theft mostly involves stealing someone's identity to make a staggering number of financial and personal transactions in someone else's name [32]. Similarly, medical identity theft also includes the stealing of patients' information for personal gains. However, medical identity theft will devastate not only the victims' finances but also the health care services the victim will receive in the future. The perpetrators may steal patients' records to sell them in the black market or they may alter patients' records (e.g.: add false entries regarding diagnosis) to claim the Medicare. Victims who have their medical records altered by the perpetrators will receive wrong medical treatment that may cause catastrophic consequences to their health. (2) Compared to financial identity theft, most of the medical identity thefts are conducted by insiders who may turn out to be the patients' relative or family members, physicians who have access to patients' records, nurses, billing clerk, lab technicians etc. In other words, medical identity theft is an insider job. (3) While the victims of financial identity thefts are presented with recovery tools to control the damages, the victims of medical identity thefts have no recourses for recovery once they discovered false entries in their medical records. Under Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules, the Accounting of Disclosure (45 C.F.R. §164.528) requires health care providers (covered entities) to maintain an accounting for disclosure and it could possibly help some victims of medical identity theft. However, there are exceptions: a covered entity is not required to maintain accounting of disclosures for treatment, payment, or health care operation. Under this circumstance, victims of medical identity theft are almost impossible to track the flow of medical information in an attempt to view the false entries created by perpetrators [9]. (4) As financial identity theft can be traced using credit reports, medical identity theft unfortunately is a hidden crime that is difficult to uncover. Financial identity theft that involves usurping someone else's credit card is very self-revealing as account holder may notice the changes in credit card statements. Nevertheless, reviewing credit report may not catch medical identity theft because what you see is never a problem [31]. Medical identity theft, indeed, is a very sophisticated crime committed by highly educated and well-trained medical employees with sophistication. Usually, the less sophisticated or greedier criminals get caught.

8. DYNAMICS OF MEDICAL IDENTITY THEFT

The root of medical identity theft is falsification of medical charts [9]. However,
falsification of medical records without abusing the bogus records is not considered medical identity theft. It merely causes data inaccuracy but it does not use the fabricated data to claim Medicare for financial gain. This crime is mostly an insider job and medical information is being stolen by organized criminal gangs [5]. The insiders who commit this crime can be health care workers such as physicians, nurses, front desk workers, billing clerks, lab technician etc. A crime is identified as medical identity theft when the false information was created by a perpetrator who used the victim's identity to obtain medical services or to generate false claims for services, as part of a scheme to commit health care fraud and receive payments for services never provided [23]. For instance, one group optometry practice sent salespeople to the director of nursing or social worker at different nursing facilities to offer routine eye examination for all patients at no cost. The nursing staff provided access to patients' records and the Medicare was billed

for all kind of other services that were provided [31]. The preceding example shows that medical identity theft is committed by insiders and victims are mere a commodity in the eyes of the perpetrators.

Other than insiders' access to patients' records, identity thieves may obtain information by [7]: (1) accessing information based on a legitimate need and then distributing the sensitive information for criminal purposes; (2) hacking into computerized patient information; (3) dumpster driving or collecting information from organization's trash or recyclables; and (4) stealing wallets, purses, or mail from patients, visitors, or staff.

9. NEGATIVE IMPACTS OF MEDICAL IDENTITY THEFT

According to World Privacy Forum [9], Medical Identity Theft has profoundly and adversely impacted the victims in the following ways:

- Victims may experience the familiar consequences of financial identity theft that can include loss of credit, harassment by debt collectors, and inability to find employment.
- False entries in victim's medical record may remain in victim's medical files for years and may not be corrected or even discovered. There is seriously lack of recourse for victims to make amendment to the falsified and inaccurate medical records. HIPAA rules do not mandate health care providers that did not create a falsified record correct the falsified entry.
- Alteration of patients' medical records will reflect inaccurate medical conditions, blood types, drug allergies, and other health information relied upon to administer medical care. False entries in victim's medical record may cause the victims to receive wrong medical treatment. This is most egregious crime because inaccurate medical record can kill a patient.
- Victims may find their health insurance exhausted, and become uninsurable for both life and health insurance coverage.

10. DETECTION OF MEDICAL IDENTITY THEFT

Given that medical identity theft is a crime that hides well, victims usually discover it at some very unpleasant moments, such as getting rejected of health care insurance and employment opportunities. Victims always discover this crime after it has occurred for a considerable amount of time. Very few literatures provide suggestions on how to proactively detect medical identity theft before it inflicts serious damages upon the victims. The following depicts how the victims of medical identity theft detect the crime:

- Collection notices: perpetrators change the billing address and the phone numbers on the medical charts of victims. This will make it hard for the bill collector to find the victims. If the perpetrators are not very sophisticated, the victim received letter from collection services to demand the victim to pay for the medical treatment that he or she never received.
- Credit report: consumers whose medical identity was stolen and used to open multiple credit card accounts will be able to detect this crime after reviewing their credit reports. However, most of these crimes are committed by educated, sophisticated perpetrators who know how to hide crimes well.
- Receipt of someone else's bills: A less sophisticated criminal will create medical bills that can tip victims off.
- Notification by law enforcement or an insurance company: victims may be contacted by an insurance fraud investigator or law enforcement regarding crime.
- Notification by a health care provider: it is very unusual for health care provider, such as a doctor or a hospital, to notify the patients of medical identity theft. However, there have been a few cases reported by hospital when the discrepancies in the medical records are discovered.
- Medical problem at an emergency room: the most unfortunate thing is that victims learn about medical identity theft during the course of medical emergency. Most often, victims spot false entries in their medical records.
- Denial of insurance coverage, notification that run out, or "lifetime cap" has been reached: this is another way for victims to discover medical identity theft. Victims may be notified that the coverage for their medical services is being denied because their benefits have been depleted.

11. PREVENTION OF MEDICAL IDENTITY THEFT

This research paper outlines preventive steps after analyzing data in multiple case studies. Currently, literature reviews provide background knowledge on this subject matter. An identity theft literature, Identity Theft and Fraud – the Impact on HIM Operations, outlines the practical preventive guidance:

- Ensure appropriate background checks of employees and business associates who may have access to the patient protected health information.
- Minimize the use of social security numbers for identifications whenever possible and avoid displaying the entire social security numbers on the computer screens, documents or data collection fields.
- Store patient protected health information (PHI) in a secure manner by enforcing physical safeguards (e.g.: use restricted areas or locks).
- Implement and comply with organizational policies for the appropriate disposal, destruction, and reuse of any media used to store and collect patient protected health information (PHI).
- Train staff on organizational policies and practices to provide protection and appropriate use and disclosure of patient protected health information (PHI) as well as appropriate ways to handle identity theft events.
- Develop a proactive identity theft response plan or policy that clearly delineates the response process and identifies the organization's obligations to report the crime.

12. POLICIES AND PROCEDURES AND SECURITY CULTURE

Implementing policies and procedures to protect patients' data from medical identity theft requires not only sound management skills but also a culture of security awareness. Security culture embodies all socio-cultural measures that support technical security measures, so that patients' information security becomes a natural aspect in the daily activities of every employee [28]. The importance of security culture becomes apparent when much of the security problem is not of a technical-only nature but of a cognitive and organization nature, as well [16]. The formulation and implementation of a security policy and procedures draw on the existing culture, norms and rules and have the potential to affect them and therefore these processes can have an impact on the social context [18]. On the bright side, culture presents a common language to foster the understanding of policy and procedure and helps to enforce the security practice. Otherwise, culture can eat technology for lunch. In other words, culture decides whether to espouse or eschew security practice. The components of security culture are shown below:

1. Attitude and Awareness

The attitude of the given societal environment, regarding enforcement of security rules.
The awareness of the societal environment, regarding security issues in general.
The attitude of the relevant professional community towards enforcing security rules [19].

2. Power Relation between Users

The exercise of power by health care professions affect the implementation of policy and procedure.
Political perspective: the ability of health care professions to affect an outcome and to get things done.

3. Collective Norms, Values, and Knowledge

The introduction of new rules and interpretation schemas can be in accordance or in conflict with the pre-existing ones, therefore altering the way people perceive things and thus creating new norms and patterns of practice [18].

The context in which a security policy is formulated and eventually put to practice is characterized by certain rules, norms and interpretation schemes [18].

Reluctance to change working practices in order to make information more secure among health care professionals can be an impediment to the implementation of policy and procedure [15].

4. Assumptions and Beliefs

The organization values shape the underlying assumptions and beliefs that influence the security culture.

In regard of medical identity theft, health care professions must be aware of the ethical issues and security practices in health care environment. Many health care professions are unaware of the security threats across the integrated network delivery system that involves multiple third parties. The security awareness will become more important after the implementation of the proposed National Health Information Network (NHIN). The United States Department of Health and Human Services (HHS) envisages that by placing health records online and making health records available everywhere, NHIN will save lives and reduce frauds [9]. However, without proper safeguards and appropriate administration supported by a culture of security, NHIN will run the risk of malicious attack and information theft. In the realm of data security breaches, technology itself is not the culprit but poor enforcement of health care policies due to a lack of security culture is. The result of the research will shed lights on how to coordinate health care policy and procedure with security awareness.

13. RESEARCH METHOD

1. Qualitative Positivist Approach

A qualitative positivist approach is adopted. The key feature of qualitative positivist research method emphasizes on the scientific adoption of positivist approach (e.g.: theory testing, hypothesis testing, formal propositions, inferences making etc.) to attain a better understanding of a phenomenon from the participants' view points. Qualitative positivist research method can be used for the exploration, classification, and hypothesis development stages of the knowledge building process [2]. This approach is well suited to capturing the knowledge of practitioners and developing theories from it; and the knowledge can later be formalized and brought to the testing stage [2]. Given that, qualitative positivist approach is suitable for this research topic because I would like to use case studies to capture a health care phenomenon in a natural setting and then collect data or empirical materials to draw inferences to explore the issue of medical identity theft, a topic that is less researched and studied.

14. PURPOSE OF CASE STUDIES

In health care research, case studies encompassed knowledge pertaining to technology utilization, medical and organizational innovations, and the implementation of specific health legislation, policies, and programs [33]. The need for case studies arises when an empirical inquiry must examine a contemporary phenomenon in its real life context especially when the boundaries between phenomenon and real life are not clearly evident [34]. In this regard, the primary purpose of the case studies is to explore and explain the insider job aspect of medical identity theft (phenomenon) in a natural health care setting (context). Case studies can be employed to develop and to test a theory through induction [6]. Given that medical identity theft is a new topic, this theory isconstructed from a case study so as to start from a clean theoretical slate. Theory-building research stems from the notion that there is no theory under consideration and no hypotheses to test [11]. Another viable option is running hypothesis testing or theory testing. Lee [20] has posited that when using case studies to test theories, natural science model can incorporated to make controlled observation, make controlled deduction, allow for replicability, and allow for generalizability. Finally, proposing multiple case studies for theory-building purpose to address that there are very few theory-building researches in this topic according to the available literatures. Not many insights are offered to explain the insider jobs of medical identity theft. Hence, it makes sense to build theory based on the findings and discoveries.

15. CASE STUDY DESIGN

1. Multiple Case Studies

Regarding this research topic, multiple case studies are used because (1) multiple case studies provide the opportunities for juxtaposition of all the cases. Cross case research analysis prevents the researchers from jumping to conclusion by allowing researchers to draw juxtaposition to search for patterns and counteract the tendencies by divergently looking at the data; (2) multiple case studies permit researchers to conduct cross-case analysis that lists the similarities and differences between cases and

subsequently makes the researchers look at the subtle similarities and differences. This enables researchers to break simplistic frame, leading to sophisticated understanding [11]; and (3) case studies can be used for both exploratory and explanatory purposes. For example, the first case study will explore medical identity theft in the natural health care setting. After data collection and data analysis, the second case study will be carried out. The earlier case may produce certain facts in which its significance was only realized after a subsequent case has been completed and the reinterpretation of facts in the subsequent case facilitates the materialization of a more general explanation across all the cases [34]. This will achieve the purpose of exploring and explaining medical identity theft.

2. Operational Framework

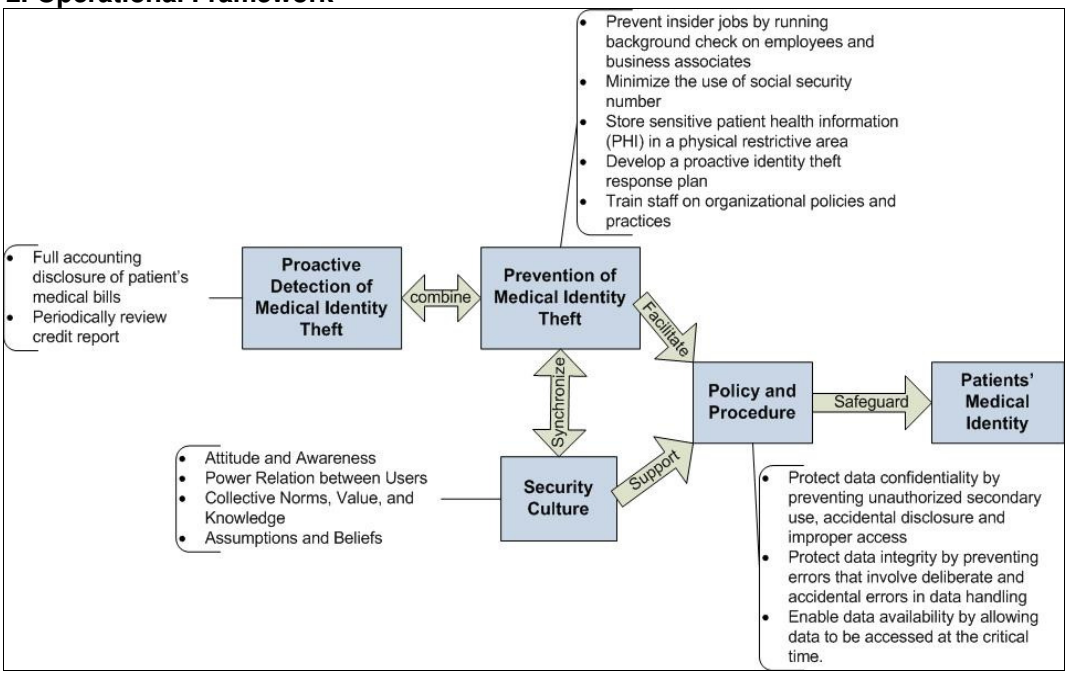

FIGURE 1: A Detailed View of Operational Framework (Baker, Verizon 2010)

The two case studies are conducted in two different health settings – Northern Michigan Hospital and Emmet County Health Care Department. Several constructs, as shown in figure 1, are outlined tentatively. The constructs demarcated are based on the findings from literature reviews. The framework above is a logical model that shapes the priorities for exploring in this case study research. Yin [35] postulated that good case studies should contain some operational framework; and having an operational framework prior to the inception of a case study helps to define what is to be studied as well as the topics or questions might have to be covered. The operational framework defined may inadvertently create biases but the framework itself is not a rigid design. Realizing that multiple case studies will unveil different findings, the framework will be modified to reflect the significant findings and discoveries. For instance, more constructs will be added or an existing construct will be better defined. Flexibility and the possibility of discovery have already been taken into consideration. In case study research, flexibility allows researchers take advantage of the uniqueness of a specific case and the emergence of new themes to improve the existing framework and resultant theory [11].

16. DATA COLLECTION

Typically, theory-building researchers combine multiple data collection methods [11]. Therefore, in these theory-building case studies, multiple data collection methods from multiple sources will be combined to make use of triangulation in support of construct validity. Medical identity theft victims and health care practitioners were interviewed wherethe interview questions were open-ended and all the interviews were recorded and transcribed to word processor, with interview date and time.

1. Interview questions that involve the victims will encompass:

- The process of identifying medical identity theft
- The time frame of detecting medical identity theft
- Steps taken to notify the health care providers
- Any help offered by the health care providers
- The repercussion of medical identity theft to the individual

2. The interview questions that health care practitioners or administrators participated are as follows:

- Approximately how many times did the victim contact the health care providers
- What are the response given to the victim
- What steps have been taken by health care administrator to rectify the situation

Other than interviews, different data collection methods were utilized, such as questionnaires, documentations, and direct observations. Both qualitative and quantitative data were collected in this case study research. Quantitative data can indicate relationships that may not salient to the researcher whereas qualitative data is useful for understanding the rationale revealed in quantitative data [11].
In summary, the following depicts different data collection methods:

17. DATA COLLECTION

1. Questionnaires	The main purpose of the questionnaire is to find out whether the health care employeesare aware of the security policies and whether they support the policies [28]. The questions serve to measure the security attitude and perception of employees.
2. Documentations	Health care settings have a staggering number of documents and forms that require research attention. This is because documents usually show the operationsand events in health care settings over a period of time. This method allows researchers to keep records of exact references and details of events. In specific, this method allows us to study the existing policies and proceduresand technological application in a health care setting.
3. Interviews	Unstructured interviews will be conducted with health care professionals and victims of medical identity theft. Interviews are necessary to directly focus on the victims' andhealth care workers' perspective.
4. Direct Observation	Health care workers may not reveal their true value in questionnaires or interviews.The objective of direct observation is to compare the answer given during interviewwith their real behavior.

The challenge of multiple resources of data collection is that it may be hard to attain convergence information [34]. Given an array of evidence gathered, it is essential to determine whether evidences from different sources converge on a similar set of facts [34]. One of a good way is to investigate. For example, through an informant (health care administrator) most of the health care workers strictly adhere to HIPAA regulations for the purpose of safeguarding personal health information. Through direct observation, the investigator may discover that copies of health care records with Medicaid ID and patients' social security number are left unattended and this practice has continued for several days. This will disconfirm the information provided by informant and the convergence information will reveal that health care workers in the health care setting do not take necessary actions to safeguard personal health information.

18. VALIDITY AND RELIABILITY

The proper use of case study protocol indicates reliability [6],[35]. Given that, the protocol refers to sequential design in multiple case studies. The first case study, as indicated in the preceding section, was conducted in Northern Michigan Hospital. There are two rounds of data collection for each case study. The second round of data collection will serve the purpose of filling the information gap but not for

longitudinal reasons. The final case analysis for the first case was written after the second round of data collection. Next, a subsequent case study was carried out Emmet County Health Care Department. The final analysis for each case will be compared and further analyzed. Construct validity can be enforced by sharing the collected data and research findings with the informants and getting feedback from the informants [6]. Although the informants may disagree with the findings, they will point out the incorrect data, if any. The purpose of using sequential design is to allow for reinterpretation with the facts of the earlier case and apply general explanation across all cases [34]. Given that, multiple case studies will serve both exploratory and explanatory purposes.

1. Data Analysis

Case studies research will yield a tremendous amount of data. Breaking the data by data source is a good way to handle a staggering amount of data. For instance, data collected from interviews and data collected from questionnaires independently was reviewed independently. This is to separate the qualitative data analysis from quantitative data analysis. It is important to keep in mind that qualitative data provides insights about the underlying issue of medical identity theft in a dynamic environment. There is anticipation that new variables will emerge as a result of serendipitous changes in the dynamic environment. The predefined constructs may have to iterate between constructs and case data to redefine the operational framework that serves as guideline in this case study.

19. RESULT/CONCLUSION

Attitude and perception of employees towards security has been discovered through the results of questionnaire. Descriptive statistic will be applied in data analysis of the questionnaire to give us a clue pertaining to security awareness in health care organization. This piece of information will then be integrated with qualitative data that will provide us the insight of prevention and detection of medical identity theft. The qualitative data will embody data collected from interviews, documentations (e.g. health care records), and notes taken from direct observation. In summary, the following table depicts research results:

1. Questionnaire	Descriptive statistic will yield result that will shed light on the security culture of a health care organization.
2. Interview	Data collected from interviews will produce result regarding the insights of medical identity theft, including how it occurred, the way health provider handled this issue, and the negative ramification on the victims.
3. Documentation	Documentation will include meeting minutes, medical forms, billing forms, and health record. The result will provide insights about organization structure and the operation issue within a health care organization.
4. Direct Observation	The result of direct observation will be able to capture part of the organization culture and attitude towards security.

The results from every type of data collection will be integrated to shape a holistic view of medical identity theft. In specific, the incident of medical identity theft can be viewed from organizational, operational, technology, and human resource perspectives [12]. This holistic view will facilitate proper suggestions of health care policies and procedures and build theories regarding medical identity theft. Most likely, multiple theories will be derived from multiple case studies. These theories will involve several variables including detection and prevention of medical identity theft, health care policies and procedure, security culture, and technology application.

Cross case analysis will point to contradicting facts. There is strong evidence indicating a lack of security culture in one case study and strong security culture in another.Thisoccurrence caused addition of technology as a new construct in the operation framework, inferring that technology plays a role in fighting medical identity theft.

A juxtaposition of multiple case studies will reveal subtle similarities and differences. For example, both case studies show that the incidents of medical identity theft were committed by medical billing specialists. The victim in a case study discovered the crime through inaccurate billing whereas the victim in another case study discovered the crime through inaccurate medical data that was unveiled when the victim was admitted to the hospital for surgery. The difference may infer that the perpetrator in the later case study was much more sophisticated than that of the former case. Pro-active detection of medical identity theft, in this regard, will encompass reviewing both medical billing record and patient's medical data [4].

Macroscopically, the resultant theories from these case studies will suggest proactive detection and prevention of medical identity theft and recommend sound policies and procedures to mitigate the risks of security breaches in health care information systems. This will also provide suggestion to reduce security risk in the proposed National Healthcare Information Network (NHIN).

20. FUTURE RESEARCH

The future research will test new theories formed in multi case studies. Given that, the next action will be shaping hypotheses by comparing the relationship with each case study to see how well it fits with case data. The hypotheses-shaping process will also involve sharpening of constructs that will encompass refining the definition of the construct and building evidence that measures the construct in each case.

REFERENCES

1. Appelbaum, P.S., "*Threats to the Confidentiality of Medical Records – No Place to Hide*", JAMA; (283:6), pp. 795-797, Feb 2000.

2. Benbasat I., Goldstein D.K., and Mead M.,*"The Case Research Strategy in Studies of Information Systems"*, MIS Quarterly; (11:3), pp. 369-386, Sept. 1987

3. Biotech Business Week, "*Electronic Medical Records: Medical Identity Theft Survey Shows Consumers Concerned about Privacy, Protection of Records*", Jan 8, 2007.

4. Boyd, A.D., Hosner, C., Hunscher, D.A., Athey, B.D., Clauw, D.J., and Green L.A., *"An Honest Broker" mechanism to Maintain Privacy for Patient Care and Academic Medical Research"*, International Journal of Medical Informatics; (76); pp. 407-411, 2007,.

5. Conn, J., *"A Real Steal. Patients, Providers Face Big Liabilities as Medical Identity Theft Continues to Rise, and in Many Cases it's an Inside Job,"Mod Healthc;* (36), pp. 26-28, 2006.

6. Cooper, R. B., *"Information Technology Development Creativity: A Case Study of Attempted Radical Change"*, MIS Quarterly; (24:2), pp. 245-276, Jun. 2000,.

7. Davis, N., Leniery, C., and Roberts K.,"Identity Theft and Fraud – The Impact on HIM Operations", Journal of AHIMA; (76:4); April 2005.

8. Davenport, K.A.,"*Identity Theft that can Kill you*", Available at www.law.uh.edu/healthlaw/perspectives/2006/(KD)**IdentityTheft**.pdf

9. Dixon, P., *"Medical Identity Theft: the Information Crime that can Kill You*", The World Privacy Forum; May 2006.

10. Earp, B.E. and Payton, F.C.,*"Information Privacy in the Service Sector: An Exploratory Study of Health Care and Banking Professional"*, Journal of Organizational Computing and Electronic Commerce; (16:2), pp. 105-122, 2006.

11. Eisenhardt, K.M., *"Building Theory from Case Study Research"*, Academy of Management. The Academy of Management Review; (14:4), Oct 1989; ABI/INFORM Global.

12. Emam, K. E., Neri, E., and Jonker E., *"An Evaluation of Personal Health Informations Remnants in Second-Hand Personal Computer Disk Drives"*, Journal of Medical Internet Research; (9:3); 2007.

13. Fromer, M.J.,(2007) "*Medical Identity Theft: Under-reported, Underresearched, & More Common than Generally Known*", Available atwww.oncology-times.com; Jan 5, 2007.

14. Garson, K. and Adams C**.**, "*Security and Privacy System Architecture for an e-Hospital Environment"*, ACM International Conference Proceeding Series; (283pp. 122- 130,); 2008.

15. Gaunt, N., *"Practical Approaches to Creating a Security Culture"*, International Journal of Medical Informatics; (60); pp. 151 – 157, 2000.

16. Gostin, L.O., *"Personal Privacy in the Health Care System: Employer-Sponsored Insurance, Managed Care, and Integrated Delivery Systems"*, Kennedy Institute of Ethics Journal, (7:4), pp. 361 – 376, 1997.

17. Hutson, T**.**, "*Security Issues for Implementation of E-Medical Records*", Communication of ACM; (44:9), Sept. 2001.

18. Karyda, M., Kiountuzis, E., and Kokolakis, S**.**, *"Information Systems Security Policies: A Contextual Perspective"*, Computer & Security; (24); pp. 246-260, 2005.

19. Kluge, E. W., *"Fostering a Security Culture: A Model Code of Ethics for Health Information Professionals"*, International Journal of Medical Informatics; (49); pp. 105 – 110, 1998.

20. Lee, A. S**.**, *"A Scientific Methodology for MIS Case Studies"*, MIS Quarterly; (13:1), pp. 33-50 , March 1989.

21. Lindberg, D.A.B. and Humphreys, B.L**.**, *"The High-Performance of Computing and Communications Program, the National Information Infrastructure, and Health Care"*, Journal of the American Medical Informatics Association; (2:3), pp. 156-159, May-Jun. 1995.

22. Malin, B., *"A Computational Model to Protect Patient Data from Location-Based Re-Identification"*, Artificial Intelligence in Medicine; (40:3); pp. 223-229, Jun. 2007.

23. Merisalo, L.J**.**, "*Medical Identity Theft*", Aspen Publishers; (17:9); June 2008.

24. McMurray, A.J., Gilbert, C.A., Reis, B.Y., Chueh, H.C., Kohane, I.S., and Mandl, K.D., *"A Self-Scaling, Distributed Information Architecture for Public Health, Research, and Clinical Case"*, Journal of American Medical Informatics Association, (14); July – Aug. 2007.

25. Offen, M.L., "*Health Care Fraud*", Neurologic Clinics, (17:2); May 1999.

26. Pear, R. (2008)"*Agency Sees Theft Risk For ID Card In Medicare", Available at* www.nytimes.com/2008/06/22/washington/22medicare.html

27. Roger France, F.H**.**, "*Control and Use of Health Information: a Doctor's Perspective*", International Journal of Bio-Medical Computing, (43); pp. 19-25, 1996.

28. Schlienger, T. and Teufel, S., *"Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture"*, Proceedings of the 14th International Workshop on Database and Expert Systems Applications; 2003; IEEE.

29. Sloane E.B., "*Using Standards to Automate Electronic Health Records (EHRs) and to Create Integrated Healthcare Enterprises*", Proceedings of the 29th Annual International Conference of the IEEE EMBS, Aug. 2007.

30. Smith, E., and Eloff J.H.P**.**, "*Security in Health Care Information Systems – Current Trends*", International Journal of Medical Informatics, (54); pp. 39-54, 1999.

31. Sparrow, M. K., *"License to Steal. How Fraud Bleeds America's Health Care System*", Westview Press; 2000. ISBN: 0-8133-6810-3.

32. Vacca, J.R., "Computer Forensics: Computer Crime Scene Investigation, Second Edition", Charles River Media; 2005. ISBN: 1-58450-389-0.

33. Yin, R. K., *"Enhancing the Quality of Case Studies in Health Services Research",* Health Services Research (34:5), pp. 1209-1224, Dec. 1999.

34. Yin, R. K**.**, *"The Case Study as a Serious Research Strategy"*, Science Communication; (97:3), 1981.

35. Yin, R.K., "*Case Study Research: Design and Methods"*, (2nd ed.), Sage, Newbury Park, CA, 1994.