Exploring Medical Identity Theft

by Desla Mancilla, MPA, RHIA, and Jackie Moczygemba, MBA, RHIA, CCS

Abstract

The crime of medical identity theft is a growing concern in healthcare institutions. A mixed-method study design including a two-stage electronic survey, telephone survey follow-up, and on-site observations was used to evaluate current practices in admitting and registration departments to reduce the occurrence of medical identity theft. Survey participants were chief compliance officers in acute healthcare organizations and members of the Health Care Compliance Association. Study results indicate variance in whether or how patient identity is confirmed in healthcare settings. The findings of this study suggest that information systems need to be designed for more efficient identity management. Admitting and registration staff must be trained, and compliance with medical identity theft policies and procedures must be monitored. Finally, biometric identity management solutions should be considered for stronger patient identification verification.

Key Words: Medical identity theft, patient identification, admitting, registration compliance

Introduction

The crime of medical identity theft is a rising concern in healthcare institutions. Medical identity theft is defined as "when someone uses an individual's identifying information, such as their health insurance information or social security number, without the individual's knowledge or permission, to obtain medical services or goods, or to obtain money by falsifying claims for medical services and falsifying medical records to support those claims."[1] The American Health Information Management Association (AHIMA) practice brief on medical identity theft cites the cascading effects of the crime and identifies potential negative financial and healthcare impacts to both individuals and public health.[2] In addition to the defrauded consumer, healthcare provider organizations and insurers assume risk resulting from medical identity theft in a variety of ways.

The purpose of this study was to examine current admitting and registration practices used in acute healthcare facilities to determine best practices that may reduce the occurrence of medical identity theft.

Background

Medical identity theft negatively affects healthcare consumers, providers, and payers. At the consumer level, healthcare and financial problems resulting from medical identity theft can have devastating effects. A healthcare consumer whose medical identity is linked with another individual's medical information could encounter life-threatening experiences as a result of receiving inappropriate medications or treatment. Consumers may suffer financial consequences when healthcare services provided to the fraudulent individual are billed to the medical identity theft victim or the victim's insurance carrier. At the organizational level, legal, financial, and public image risks occur. Consider the legal risk to healthcare providers that do not perform due diligence in trying to prevent medical identity

theft from occurring in the organization. Legal liability issues are still unclear, but recent efforts to require accounting of all disclosures, including those made to business associates or others for treatment, payment, or healthcare operations, point toward the importance of being able to send corrected information to all previous recipients of erroneous information, as is the case when someone's medical identity is assumed.[3]

Dixon suggests that the response to claims of medical identity theft in healthcare is unfavorable when compared to the more sophisticated response methods used in cases of financial identity theft.[4] Lafferty notes that over 19,000 medical identity theft complaints have been filed with the Federal Trade Commission (FTC) since 1992, while Dixon suggests there may be as many as 250,000 to 500,000 victims.[5, 6]. The number of medical identity theft claims investigated by Aetna more than doubled in the period from 2006 to 2007.[7]

In 2008, the Office of the National Coordinator (ONC) for Health Information Technology commissioned a study specifically addressing the privacy and security issues of health information exchange activities that may promote medical identity theft. The study summary noted the importance of appropriately implemented health information technology in preventing the occurrence of medical identity theft.[8] The ONC study, along with a recent FTC regulation known as the Red Flags Rules, has significantly affected healthcare provider organizations, which are now required to develop and implement written identity theft prevention programs.[9] Healthcare organizations now have a regulatory responsibility for addressing the issue of medical identity theft, though the methods used to prevent, detect, and remediate its occurrence are still unclear.

The number of medical identity theft claims is rising; however, laws and regulations addressing financial identity theft are not generally inclusive of medical identity theft. Medical privacy regulations including the Health Insurance Portability and Accountability Act (HIPAA) do not address medical identity theft and in some cases pose barriers for victims of this crime.[10] In at least one reported case, a medical identity theft victim was unable to gain access to his own medical record because the organization had determined it would be a violation of the HIPAA Privacy Rule to knowingly provide the perpetrator's information to the victim.[11] While the HIPAA Privacy Rule provides a method for consumers to request amendments to their health records, it is unclear whether the existing amendment process would be appropriate for revising records of medical identity theft victims.

With the increasing use of electronic health records, privacy advocates fear an increase in medical identity theft.[12] The use of e-health technology for providing medical services to remote areas will increase demands for stronger internal management practices to accurately establish patient identity before service is provided. Moreover, evidence suggests that healthcare employees and providers are frequently involved with committing or enabling medical identity theft.[13]

Research Question

The research questions for this study include the following: Is patient identity confirmed during the admission and registration process for every patient visit? What methods are used to establish patient identity at admission and registration?

Methods

This mixed-method study focused on the practices related to establishing and confirming patient identity during the admission and registration process.

Sample

The population of interest for this study was chief compliance officers in acute healthcare facilities. The sample frame consisted of chief compliance officers who were members of the Health Care Compliance Association (HCCA).

Web-Based Survey

A search was conducted to locate a validated survey tool; however, no previously validated tool was found. This is not surprising given the exploratory nature of the study. A Web-based survey with questions related to the objectives of the study was developed. The survey tool was tested with four participants, revisions were made, and the survey was finalized based on the pilot testers' feedback. The survey questions are shown in Appendix A. Data were collected using the Web-based survey tool mrInterview, which has a sample-management component that tracks respondents.[14] Tracking information was not available to the researchers, thereby protecting the respondents' anonymity.

Telephone Interviews

All survey respondents were asked if their facility had an established multidisciplinary plan related to medical identity theft. Respondents who answered yes were asked to participate in a follow-up telephone interview. Those who agreed were routed to a separate survey (to maintain confidentiality) and asked to provide their name, facility name, telephone number, and best time of contact. The investigators completed all calls using a structured interview protocol with both closed-ended and open-ended questions. The questions posed in the telephone interviews are shown in Appendix B. Both investigators participated in and took notes during all telephone interviews. The two versions of the interview notes were compared, summarized, and transcribed for future reference.

On-Site Observations

On-site observations were conducted to triangulate the data and to ensure the integrity of the self-reported survey data. The facilities were chosen from the stage two telephone respondents because they had an established multidisciplinary plan for medical identity theft and had agreed to an on-site observation. Both of the investigators visited two facilities. The investigators were nonparticipant observers. In one of the organizations, the investigators were accompanied by the organization's privacy officer. The investigators observed admitting and registration practices as unobtrusively as possible and did not interact with patients or admitting/registration personnel. The investigators conducted a frequency tally to determine how often the admitting/registration personnel followed the organization's established procedures. Field notes were taken and compiled post observation.

Results

Online Survey

In stage one, 440 HCCA members responded to the first survey. Of these, 192 were not in acute healthcare facilities and 115 were not chief compliance officers, resulting in a sample of 133 who met the criteria for participation. Because the desired sample size of 347 was not attained, all 133 respondents who met the criteria were invited to participate in the second stage of the study.

Of the 133 chief compliance officers who stated that they would participate in the second survey, 82 completed the survey. The response rate for stage one was 12.6 percent (440 of 3500) and the response rate for stage two was 61.7 percent (82 of 133). There are many explanations for the response rate for stage one. First, a sample frame is chosen to closely approximate the population. In this case, the investigators thought that the HCCA membership would be a good approximation of the population (chief compliance officers in acute healthcare facilities in the United States). This may not have been the best choice for the sample frame, and using another one might have yielded a higher response rate. Second, even though all 133 participants in stage two agreed to participate, only 82 responded even after three separate attempts were made to encourage their participation. Third, this response rate may be misleading since several of the participants responded for multiple acute healthcare facilities. In fact, 226 separate facilities were represented by these 82 responses. Fourth, the survey construct was such that some of the questions required compliance officers to confirm responses with other departments within the healthcare organization. This survey construct was necessary because medical identity theft issues are not limited to

compliance departments but are, by nature, multidisciplinary in scope. Data were downloaded from the mrInterview system and analyzed using Microsoft Excel 2007.

Survey participants were asked if proof of patient identity is confirmed at registration or admission, and participants who responded affirmatively were then asked what type of proof was used. While there were 82 total survey respondents, only 79 responded to the specific questions addressed throughout the remainder of this report. Of the 62 (78.5 percent) facilities who stated that patient identity is confirmed at admission or registration, 57 (91.9 percent) used a driver's license, while none used a biometric identifier. Twenty-three (37.1%) chief compliance officers stated that their facility used another form of proof. Respondents were asked how exceptions (other than in the emergency room) are handled if the patient arrived without proof of identity. Over half (59.5 percent) of the responding facilities stated that they provided the service anyway, while 16 percent rescheduled the service. (Those rescheduling the service include two who reported that their policies do not require proof of identity and one who reported not knowing whether proof of identity is required.) Sixteen (20.2 percent) chief compliance officers stated that they handle the exceptions using another method but were generally unsure how exceptions are handled or whether a firm policy was in place.

The next series of questions also related to registration and admission processes. The first question asked if these processes were performed face to face, with 56 (70.9 percent) of the respondents stating yes. The 21 (26.6 percent) of participants who responded "no" and the 2 (2.5 percent) of participants who responded "don't know" were asked if patient identity is confirmed at the point of care if registration/admission takes place online or via telephone. Twelve of the 23 (52.2 percent) said yes and were asked to state how they confirmed identity. Most sites (83.3 percent) indicated that they used some sort of photo ID at registration and admission. Responses to questions about biometric confirmation of identity for on-site registration or e-health services indicated that this type of technology is not currently used in practice.

Telephone Interviews

In the first stage of the survey, 46 of the 82 respondents indicated that their organization had policies and procedures on medical identity theft or financial identity theft. Of those 46 respondents, 25 (54.3 percent) agreed to participate in a follow-up telephone interview. Nine of the 25 respondents agreeing to participate in telephone follow-up completed the interview. Each telephone follow-up interview was transcribed to identify themes. The investigators used the grounded theory approach to identify themes and patterns resulting from the telephone interviews. Of the nine telephone follow-up interview participants, five provided copies of their organization's medical identity theft policies and procedures. The following themes gleaned from the telephone surveys related to identification verification practices in admitting and registration departments were identified.

Theme One: Most cases of medical identity theft come through the emergency department.

The majority of telephone survey respondents noted that emergency departments are obligated to provide treatment in most emergency cases. Respondents indicated that drug-seeking behavior and the presence of law enforcement officials in emergency departments may compel certain patients to commit medical identity theft to avoid potential arrest for other, unrelated crimes.

Theme Two: Organizations are beginning to use photographic identification storage in information systems.

Some organizations are starting to implement photo identification storage in their information systems. However, the current state of this technology is fragmented, especially when trying to implement photo identification storage across large-scale healthcare delivery systems.

Theme Three: Time constraints in admitting and registration departments may result in lack of compliance with organizational policies and procedures related to identification verification.

The admitting and registration staff is often unskilled in the detection of falsified identity documentation. These positions are typically clerical in nature, and employees are under time constraints to quickly process patients' registration for healthcare services, giving them little time to fully consider potentially fraudulent identification documents.

Theme Four: Biometrics are a potential solution but lack consumer support and are perceived to be too costly for most healthcare organizations to implement.

Biometrics are a desirable solution for authenticating patients and ensuring that patients receiving services are the individuals they claim to be. However, providers are faced with challenging issues such as cost and consumer acceptance.

Theme Five: Widespread use of the Social Security number throughout the healthcare continuum, often starting at admitting and registration, must be reconsidered in order to further reduce the occurrence of medical identity theft.

As part of the internal risk assessment for medical identity theft, many organizations are carefully monitoring the use of the Social Security number in clinical reports, applications, and information systems. Participants noted that a Social Security number is considered to be extremely valuable to an identity thief. One respondent noted that organizations have been much too cavalier about the use of the Social Security number.

On-Site Observation Visits

Five of the telephone interview participants were asked if they would allow the investigators to conduct an on-site observation of patient registration processes. The investigators visited two academic medical centers in geographically disparate locations in order to observe employee compliance with the organizations' policies and procedures related to verification of patient identity at the time of registration or admission. The intent of the on-site observations was to verify actual practices and to compare them to the organizations' policies and procedures related to verification of patient identity at admitting and registration. Five inpatient admissions, one emergency department registration, and 30 outpatient clinic registrations were observed. The policies and procedures for identification verification varied between the two sites as well as between inpatient and outpatient service types within each organization.

Inpatient Admitting Practices

In both organizations, healthcare consumers being admitted as inpatients are required, by policy, to present a driver's license or other form of photographic identification. Both organizations' policy is to provide treatment regardless of whether the patient is able to produce photographic identification or not.

Of the five observed inpatient admissions, four consumers were asked to produce photographic identification. The one consumer who was not asked to produce a photographic identification was known to the admission associate from a previous healthcare registration. This raises the question of whether complacency may exist when registration staff are familiar with patient faces and/or names from previous patient encounters. Other notable observations and conclusions made by the investigators during the inpatient observation process include the following:

1. Consumers whose inpatient admissions are planned are told to not bring anything with them when they come to the hospital for service. Some consumers interpret this to include identification, resulting in lack of ability to confirm identity at the point of admission.
2. Admitting staff are challenged by organizational requirements to complete the admitting process quickly.

3. Photographic identification presented by consumers may not accurately depict the current appearance of the individual, thereby making it difficult for admitting staff to confidently confirm patient identity through photographic means.
4. Compliance with the policy to ask all consumers to show photographic identification at the time of admission varies.

Outpatient Registration Practices

The two observation sites' policies on photographic identity verification varied from one another in that one organization required photographic identification for registration and the other did not. As with inpatient admissions, both organizations provide service regardless of the consumer's ability to produce photographic identification. The policy within the organization that does request photographic identification is that all new patients are asked to show photographic identification, which is scanned into the organization's registration information system. Consumers arriving for repeat encounters are not asked to produce identification because the procedure directs the registration employee to compare the scanned image in the registration system to the individual who is present. A lack of compliance with this procedure was observed, with the investigators noting that out of 20 repeat encounters, none was confirmed by looking at the previous scanned image. Instead, registration associates verbally asked patients to confirm address or other identifying information. Notable observations and conclusions drawn by the investigators during the outpatient registration observation process include the following:

1. The information system design did not support efficiency in registration activities, with the photographic scanned image requiring staff to navigate through several additional screens.
2. A lack of registration staff compliance with the organization's stated policy on confirming repeat consumers' identity was noted.
3. Registration staff training on the policies related to identification confirmation varied among employees.

Emergency Department Registration

During the observation period in the emergency department, only one patient was registered, and this occurred at the bedside due to the emergent health status of the patient. Because only one registration occurred during the observation period, the investigator asked the associate to describe a nonemergent registration process. The associate gave a detailed explanation specifically including that the patient is asked to show a driver's license, with follow-up requests for other forms of identification. The associate also mentioned that in the emergency department the patient receives service regardless of the ability to prove identity.

Discussion

The primary healthcare market continuum is affected by the potential for corrupt data that may create a health and financial risk to individuals, payers, and providers. The integrity of data held by reporting and research agencies, public health agencies, and others is also suspect as a result of medical identity theft.[15]

The findings from this investigation suggest that acute healthcare providers are implementing new policies and procedures to address the rising incidence of medical identity theft, as well as comply with the FTC's new Red Flags Rule. The follow-up telephone interviews revealed that the facilities believe the majority of medical identity theft cases come through the emergency room. This highlights a potential conflict between the FTC rules and the Emergency Medical Treatment and Active Labor Act (EMTALA) of 1986 requiring acute care facilities with emergency rooms to treat all patients or face losing all federal funds, including Medicare payments.

Both the interviews and the observations indicate that admission and registration work processes, as well as their supporting technology, have not been sufficiently revised to enable the smooth implementation of the organizational policies and federal regulations designed to reduce medical identity theft. In fact, this process begins prior to actual admission, when the patient is given admission instructions and told not to bring anything to the hospital.

Limitations

The following limitations should be considered when interpreting the results of this study:

1. Only corporate compliance officers that are members of the Health Care Compliance Association (HCCA) were invited to participate in this study. Generalization of the study results may not reflect the practices of the broader healthcare community.
2. Questions in the survey may have fallen outside of the scope of the corporate compliance officer. The multidisciplinary nature of the problem of medical identity theft requires input from a multitude of organizational units.
3. Without direct observation of an organization's practices, survey responses are valid only to the extent that self-reports are reliable.
4. Sample results from stage one indicated that 440 HCCA members were willing to participate in the survey. However, the criteria for participation in the survey required members to be both the chief compliance officer and employed in an acute healthcare facility. The application of these criteria reduced the sample size to 133. This represents a missed opportunity to explore the concept of medical identity theft in other organizations that were willing to participate in the study.
5. On-site observation visits were conducted only at academic medical centers, making the results difficult to extend to other types of acute healthcare organizations.
6. On-site observation results are limited by the patient activity at the time of the observations.
7. The lack of a validated survey tool and limited financial resources to conduct a full reliability and validation assessment limit the generalizability of survey results.

Implications

The implications of this study include the need for additional understanding of the challenges facing admitting and registration departments in terms of training and compliance with organizational policies and procedures. In the healthcare industry, providers need to integrate education on medical identity theft as part of new employee orientation and continue these training sessions at periodic intervals.

There is also an opportunity for providers to educate consumers about medical identity theft at the point of care. The perceived need to commit medical identity theft in emergency departments seems to suggest a lack of consumer awareness of emergency department treatment guidelines or perhaps points toward other motivating factors. Regardless of the reason, consumers should become better educated about the potential effects of medical identity theft. As acute healthcare organizations develop programs to prevent medical identity theft, the opportunity to further educate consumers will become increasingly important.

The legal and regulatory framework that guides healthcare organizations has become extremely complex in regard to medical identity theft. The Red Flags Rule, HIPAA, and even more recent language in the American Recovery and Reinvestment Act of 2009 (ARRA) have a potential impact on how acute healthcare organizations address the rising occurrence of medical identity theft. The fact that differing federal and state agency regulations apply to medical identity theft highlights the need for a coordinated approach to ensure that healthcare providers and victims are not caught in the middle.

Conclusions

The crime of medical identity theft is a rising concern in healthcare institutions. The majority of acute healthcare facilities have policies and procedures in place for identifying patients at registration/admission. However, time constraints as well as the skill level of admitting and registration personnel for detecting fraudulent forms of identification may perpetuate the problem of medical identity theft. Additionally, stronger technology support may be needed particularly in the form of biometric identification verification. The use of biometrics as a method of healthcare identification verification may become increasingly important with the growth of e-health related activities.

In order to better protect patients' medical identity, information systems should be designed to allow for operational efficiency in the patient identification verification process. Before purchase, organizations should evaluate system capabilities to assist in the detection and prevention of medical identity theft. Further, staff must be trained and compliance with policies and procedures must be monitored to effectively detect and prevent the occurrence of medical identity theft. Information systems and manual processes should also be surveyed to ascertain the current use of Social Security numbers. When possible, organizations should reduce the use of the Social Security number in both administrative and clinical documentation in order to reduce the opportunity for medical identity theft.

Finally, further research is needed to better understand contributing and preventive factors related to medical identity theft. Additionally, the authors recommend that organizations revising their policies and procedures to address medical identity theft utilize process improvement and workflow redesign principles to minimize any unintended consequences such as noncompliance or consumer frustration with conflicting instructions and expectations.

Acknowledgments

The AHIMA Foundation grant-in-aid program funded this study. The Health Care Compliance Association provided access to their member list for survey dissemination. The investigators also wish to thank Dr. Gail Ryser, director of the Texas State University Testing and Research Center, who provided valuable assistance with survey design and analysis, and Dr. Susan Fenton, who assisted with article revision recommendations. The survey respondents, the telephone survey follow-up participants, and the organizations allowing investigators' on-site observations are also acknowledged for their assistance in bringing this study to fruition.

Desla Mancilla, MPA, RHIA, the principal investigator, is the Health Informatics and Information Management Program Director at West Suburban College in Oak Park, IL.

Jackie Moczygemba, MBA, RHIA, CCS, the secondary investigator, is an associate professor in the Health Information Management Program at Texas State University in San Marcos, TX.

Notes

1. Dixon, P. "Medical Identity Theft: The Information Crime That Can Kill You." *The World Privacy Forum* (2006): 13–22.
2. AHIMA e-HIM Work Group on Medical Identity Theft. "Mitigating Medical Identity Theft." *Journal of AHIMA* 79, no. 7 (2008): 63–69.
3. AHIMA Advantage Alert. *Be Prepared for Changes in Accounting for All Disclosures*. March 25, 2009. Available at http://www.ahima.org/images/Newsletters/E-alert/03_26_09_browser.htm (retrieved April 13, 2009).
4. Dixon, P. "Medical Identity Theft: The Information Crime That Can Kill You."
5. Lafferty, L. "Medical Identity Theft: The Future Threat of Health Care Fraud is Now." *Journal of Healthcare Compliance* (2007): 11–20.
6. Dixon, P. "Medical Identity Theft: The Information Crime That Can Kill You."
7. Knight, V. "Escalating Health-Care Costs Fuel Medical Identity Theft; Patients Are Told to Guard ID Cards Like Other Plastic." *Wall Street Journal* (October 11, 2007): d3.
8. *Medical Identity Theft Final Report.* Prepared for the U.S. Department of Health and Human Services by Booz Allen Hamilton (2009). Contract number HHSP233200045008XI. Available at http://www.hhs.gov/healthit/documents/MedIdTheftReport011509.pdf (retrieved April 13, 2009).
9. Alexander, J. "Healthcare Organizations Must Have an Identity Theft Policy: FACTA or FICTION?" *Healthcare Financial Management* 62, no. 9 (2008): 38–40.
10. Dixon, P. "Medical Identity Theft: The Information Crime That Can Kill You."
11. Ibid.
12. "Diagnosis: Medical Identity Theft." *Business Week*, January 8, 2007, 30.
13. Weeks, K. "Fast Growing Medical Identity Theft Has Lethal Consequences. *San Diego Business Journal* (October 16, 2006).
14. mrInterview (Professional) version 5.5. Patch Level: 0.Copyright © 2002-2008 SPSS Ltd.
15. AHIMA e-HIM Work Group on Medical Identity Theft. "Mitigating Medical Identity Theft."

Appendix A
Web Survey Questions

1. Is proof of patient identity confirmed at registration or admission?

2. Patient identity is confirmed by the following (**Check all that apply**)

   Driver's license
   State identification card
   Biometric identifier (fingerprint, eye scan, etc.)
   Other form of identification (**List all other acceptable forms of identification**)

3. Other than in the Emergency Department, how are exceptions handled for individuals that arrive for service but do not have proof of identity? **(Checklist – Provide service, do not provide service, reschedule service, other – please specify)**

4. Are all registration and admission processes performed face to face with patients or their designated legal representative?

5. When registration/admission takes place online or via telephone, is patient identity confirmed at the point of care?

6. When online or telephone registration/admission is used, where and how is patient identity confirmed? (**Check all that apply**)

   Photo identification shown at registration or admission department
   Photo identification shown at department of service
   Biometric confirmation in online registration process
   Other (**List all other acceptable forms of identification**)

Appendix B
Telephone Survey Questions

1) Hospital bed size
2) How many acute healthcare facilities are represented in survey response
3) Hospital location
4) Does your organization have a multidisciplinary plan in place to address medical identity theft?
5) Can you describe the plan?
6) Describe to us how well your plans works. Are there any weaknesses?
7) Has your organization considered how it will handle patient identification for e-health services? If so, what mechanisms will be used?