Medical Data Breaches

Susan Fowler
Purdue University
fowler16@purdue.edu

Samuel Liles
Purdue University
sliles@purdue.edu

Abstract

Medically identifiable information is recorded, used, and stored in a variety of locations and for a variety of purposes. Several federal laws exist to give framework to policies and procedures meant to ensure the privacy and security of medical information. Even though these laws exist, breaches and leakages of medical data continue, typically, through loss or theft of mobile devices. Stolen medical information can be used for multiple nefarious reasons, including medical identity theft, which can cause patients, providers, and insurance companies to lose money, data integrity, and potentially cause harm or liability. Presenting how medical identity theft affects all the stakeholders and the amount of damage that can be committed is discussed, along with suggestions for reducing risks during various stages of the information life cycle.

Introduction

Electronic medical records are an evolving industry, with issues such as regulations, access controls, training, and policies needing to be addressed and resolved. At stake is consumer privacy and protection from issues such as theft, data breaches, loss, inaccuracies, exposure of personal data, and medical identity theft. Electronic medical records are found at insurance companies, clinics, hospitals, employers, and government agencies as well as the network that transmits and ultimately stores them. This creates a real concern regarding the integrity of electronic medical records and how they are handled during their life cycle.

While the government has implemented the Health Insurance Portability and Accountability Act (HIPAA) to protect consumers and provide regulation, the potential for compromised data remains. Upwards of 94% of healthcare entities experienced a data breach within the past two years [1], and according to the Ponemon Institute, only 40% of their healthcare provider survey respondents feel they are prepared to detect and prevent electronic medical record breaches now or in the future [2].

The goal of this paper is to provide a general overview of potential security risks and concerns for electronic medical records. How are electronic medical records vulnerable to breaches, what areas of risk exist in each portion of the lifecycle, and how can they be addressed or mitigated? Electronic medical records contain sensitive information that requires consistent controls. The primary focus is whether the present implementation of present security and privacy standards are sufficient to discover these integrity breaches.

Who Does This Affect?

Breaches of protected health data are defined as the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information" [3]. Medical data leakages and breaches can take a variety of forms compromising a variety of data. Some of these include personally identifiable patient or employee information and business-related information such as financial or marketing data. Breaches can result from theft and losses of laptops, breached servers, or simply files left unattended. Personally identifying patient information is discussed with respect to threats to privacy as well as negative consequences that may result from its loss or disclosure.

Patients/Consumers

Patients may face a range of consequences. One such consequence is being responsible for fraudulent charges for treatment obtained under the patient's identity, which results in service limit restrictions on an insurance policy. Incorrect information in a patient record that potentially threatens the health or life of a patient or negatively impacts medical decisions made with that data [4] is another consequence of a data breach. Reports of a patient being incorrectly tagged with HIV or diabetes from having their medical records assumed by people with those diseases have also occurred. A patient may have prescriptions or medical equipment requests denied if shown that those services were already obtained by another person posing as the patient [4].

Providers

Providers often shoulder the burden of fraudulent activity from fraudulent or exaggerated billing, assuming these are paid on behalf of legitimate patient activity. When the criminal activity is discovered, they are sometimes left with unpaid service bills [5].

Insurance Organizations

Insurance companies charged with covering fraudulent services or products then pass these along in the form of increased premiums and copayments [5].

Federal Agencies

Camp & Johnson report that up to 10% of health payments paid through Medicare and Medicaid are due to criminal activity. This includes medical identity theft and dishonest health care providers. Fraudulent expenditures range from 3-10%, thus translating to hundreds of billions of dollars [5].

Taxpayers

When Medicare and Medicaid beneficiaries are compromised, taxpayers shoulder the financial burden. The current estimate is that 300,000 accounts may currently be compromised and are monitored by the Centers for Medicare and Medicaid Services (CMS) [4].

Government Creates New Legislation

The federal government had pushed to implement a national network of electronic health records by 2014 as part of the American Recovery and Reinvestment Act of 2009. HIPAA, 1996, established a framework for privacy and security requiring compliance in the transmission and disclosure of certain patient data [4]. This legislation deals specifically with healthcare coverage situations, such as a worker changing or losing a job, as well as standards for transmission of personally identifiable healthcare information [5]. The privacy and security rules within HIPAA deal with ensuring that participating parties operate under standardized administrative safeguards. This includes policies and procedures as well as physical and data structure access control and integrity [5]. The Health Information Technology for Economic and Clinical Health act (HITECH) was created to give structure to protecting medical identity security and privacy. It builds on HIPAA by requiring consumer notification of any breach to HIPAA-covered information holders or third party vendors [4]. It was created as part of the American Recovery and Reinvestment Act of 2009 to press for the development and implementation of an electronic medical record framework as well as offering lucrative incentives to hospitals and practitioners for adopting electronic medical records. In addition, it extended the HIPAA breach notification requirements to covered business associates in addition to introducing new consequences for non-compliance. The Department of Health and Human Services implemented requirements of secured and unsecured health care data after HITECH was passed. It specifically requires electronic health care records to be encrypted. It also requires the destruction of unencrypted data after it is used. This requirement also extends to HIPAA covered entities and their business partners. HITECH also increased fines under HIPAA [5].

Electronic Health Records

Benefits

Electronic health records can increase the efficiency of admitting, billing, and administrating patient care [5]. Housing patient records in a central server can speed patient diagnosis, ensure continuity of patient care, and reduce medical errors and cost. It could also serve as a database to aid research in disease or drug effectiveness patterns [6].

Drawbacks

Since electronic health records exist in a digital environment, access and corruption on a large scale is always a possibility. A variety of sensitive information can be contained in a person's medical file or history, including substance abuse, sexual history, hospitalizations, illnesses, employment information, contact information, psychological or mental health information, family histories and emergency contacts [6]. Other considerations are the costs to implement and maintain systems, information inaccuracies, and the subsequent liability concerns that may result. Health care providers may also hesitate to adopt electronic health records [7].

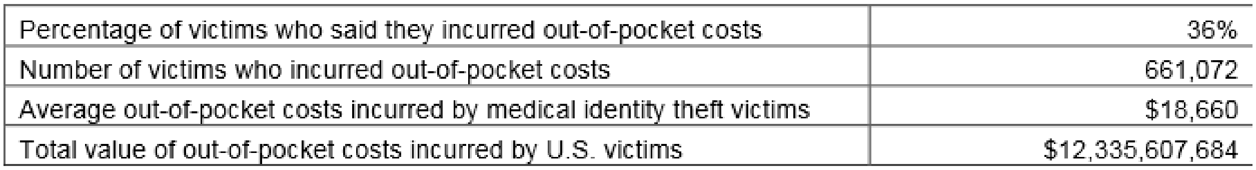
What Is the Scope of the Problem?

The Ponemon Institute reports that instances of medical identity theft are on the rise, from 1.4 million people in 2010 to 1.85 million in 2012 [2]. Conservative estimates are that 3-10 percent of all healthcare expenditures in 2012 were fraud-related. While many respondents to a medical identity theft survey reported financial losses as a result of the theft, half also reported a negative impact on their healthcare benefits or accuracy of treatment or diagnoses due to fraudulent information in their health information.

Annual Costs

These costs take various forms that may not be obvious. Costs such as identity or credit reporting services or the resulting legal counseling that may be required, additional medically necessary services or prescriptions that result from lapsing medical coverage due to policy cancellation, and paying back health care companies that fall victim to fraudulent claims or services. Table 1 shows the average out-of-pocket costs and the total consumer costs borne by consumers in 2013 [2].

Table 1. Annual projected costs of medical identity theft in the United States [2]



Percentage of victims who said they incurred out-of-pocket costs	36%
Number of victims who incurred out-of-pocket costs	661,072
Average out-of-pocket costs incurred by medical identity theft victims	$18,660
Total value of out-of-pocket costs incurred by U.S. victims	$12,335,607,684

Costs and Risks to Consumers

According to the Ponemon Institute study, it is estimated that medical data breaches cost the health care industry $6.5 billion, while the FBI estimates that health care fraud costs the U.S. economy upwards of $80 billion. The majority of medical identity theft survey participants did not understand the costs, risks, and consequences to consumers. These risks can take the form of inaccurate information in a medical file resulting in incorrect diagnoses, prescriptions, or treatment delays [2]. They also did not understand the implications of sharing medical credentials or how to reduce their chances of financial or medical consequences.

Black market value of stolen medical data is estimated to higher than that of social security numbers. Gordon reports that medical identities are traded at a rate 20 to 50 times higher than that of financial identities [8]. As financial identity theft risks and prevention have become more prominent, consumers are educated on how to protect their sensitive data, such as their social security number. This is generally not so with medically identifying data, therefore people may be less careful guarding its privacy [8]. The value of medically identifiable data will inevitably drive lawbreakers to obtain compromised data on a large scale and seek to compromise devices and systems that may house it.

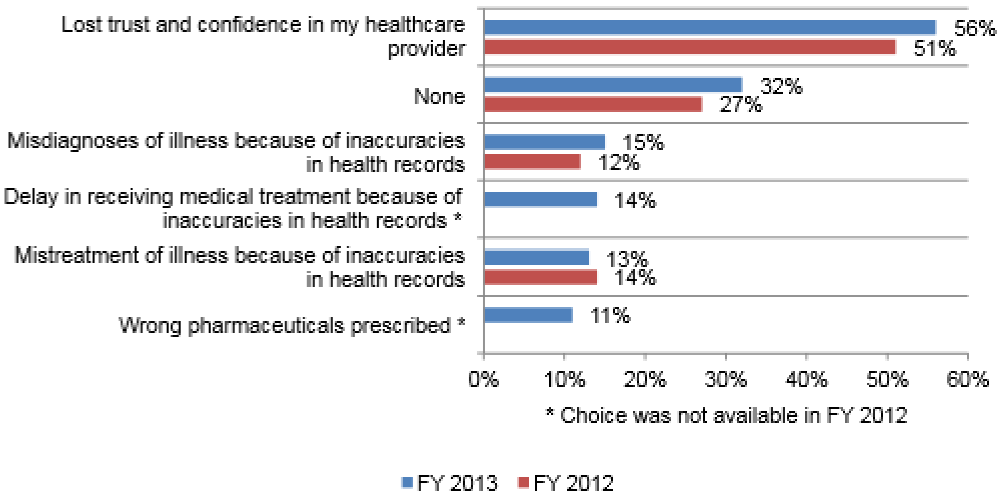


Figure 1. Percentage of respondents reporting consequences from medical identity theft [2]

Number of People Affected

The Ponemon Institute states that about 9% of the United States adult population has been victims of identity fraud, with 6% of those victims of medical identity theft. This number translates to approximately 1.5 million people [2]. The Department of Health and Human Services report that between the end of 2009 and the end of 2011, over 13,000 Medicare and Medicaid participants had their medical data breached. They reported to Congress in 2010 that over 5 million people were affected by large breaches of over 500 members at each occurrence [3]. Kierkergaard states that there were over 375 breaches resulting in almost 8 million records compromised and exposed [6]. This figure does not reflect smaller breaches of less than 500 records, as it is not required under HIPAA.

How Are the Breaches Happening?

Kierkegaard states that the 2010 HHS report to Congress noted the five top causes of breaches causing the loss of over 500 records: theft, loss of electronic or media records containing personal health information, unauthorized or inappropriate access or disclosure of personal health information, human error, and careless or improper disposal. This is especially relevant as there is no legal compulsion to report compromised or breached paper-based medical records. These records pose a distinct threat of exposure as they may contain signatures that could be used for forgery [6].

Provider-Based Records

Even with policies and procedures in place, the human factor comes into play in a wide range of ways that can compromise patient data security. Electronic eavesdropping happens when patient data is transmitted over an unsecured wireless network. Anyone within range of the network can capture unencrypted patient data with a laptop computer [4]. Health care workers can further thwart security efforts by neglecting to sign off a system session or multiple sessions on computers or devices out of their vision. These issues are compounded when used on portable or home-based health care devices [4].

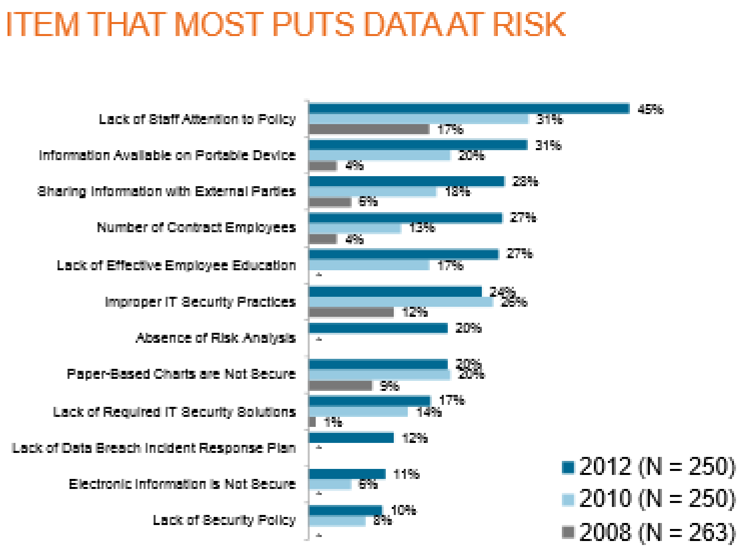


Figure 2. Kroll survey of health care entities reporting what puts data most at risk [9]

Vendors are increasingly handling or processing patient data. While Kroll reports in their provider survey that the large majority of health care providers require their vendors to sign a business agreement that outlines the vendor's compliance with HIPAA requirements, only half required those vendors to conduct periodic risk analysis to target security vulnerabilities and risks. Vendors requiring employee background checks were also roughly 50% as were those who required proof of employee training [9].

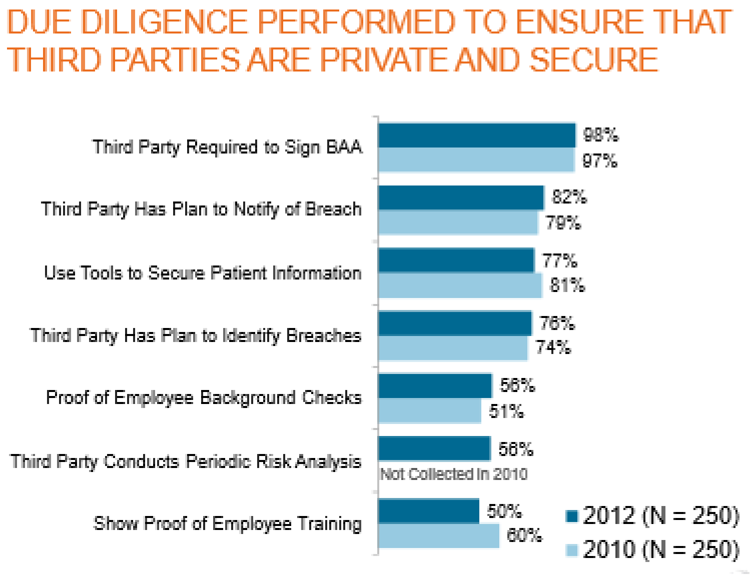


Figure 3. Survey of vendor vulnerability analysis requirements [9]

What Can Be Done with Compromised Data?

Compromised health information is also obtained within legitimate businesses practices. Past examples include "upcoding" or billing for services that were not received or exaggerated to profit [5]. Similarly, fraudulent service providers can process counterfeit or false services for stolen identities. Camp & Johnson offer an intricate example: “In one of the most aggressive recent cases, criminals combined stolen doctor entities with stolen patient identities in an elaborate long-operating fraud. Using 118 fake health clinics in 25 states, prosecutors alleged that gangsters billed Medicare for over $100 million, collecting $35 million over a four-year period” [5].

In addition to misuse, medical identities can be sold to illegal immigrants and the uninsured. These people can then use those identities to obtain care they may not have been able to otherwise afford or have access to. Drug abusers can also abuse stolen medical identities to fuel their habit or obtain prescription drugs for resale or trade [5]. Individuals who may have a criminal background or are currently wanted by the authorities are another potential market for stolen medical identities.

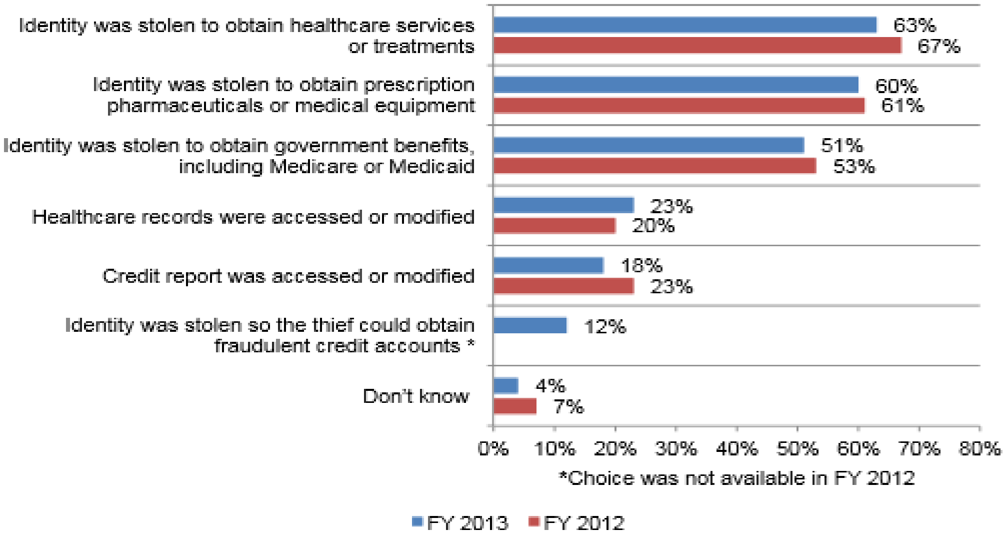


Figure 4. How the stolen information was used [2]

Medicare/Medicaid Fraud

Camp & Johnson give an example of parties hosted by criminals offering low cost medical deals in exchange for Medicaid information [5]. This information was later used to obtain reimbursement for substance and alcohol abuse counseling, complete with reports by “counselors.” These thieves were able to obtain almost $2 million dollars although no services were provided.

Medical Identity Theft

Medical identity theft deals with patient- or provider-identifying information such as social security number, prescription information, medical diagnoses and history, and insurance information. This information can be used to obtain fraudulent medical treatment or even prescription drugs and have much higher spending limits than traditional credit card fraud [5]. Worse, medical identity fraud does not have the same monitoring safeguards as financial fraud, meaning that the higher limits can be exploited with little to no oversight. In addition to the financial risks, patients may face other impacts such as difficulty discovering or removing incorrect information in their medical record. If a third party's information is contained within a patient's medical file, that information is protected under HIPAA, making detecting and removing of incorrect information all the more challenging. Other serious complications include difficulty obtaining other medical, disability or life insurance at a later date [5].

Method

Comparative methods will be used to determine how breach situations differ and what similarities are present.

Twenty-three cases of the largest HIPAA breaches in the last four years reported 74% lost/stolen data, 48% containing unencrypted information [3].

Discussion

While HIPAA can be used to prosecute or fine offenders, it is currently not widely implemented [5]. Non-HIPAA-covered vendors of personal health records are governed by the Federal Trade Commission [6], but no specific agency is in place to detect this activity, investigate, or prosecute medical identity theft [5].

What Can Be Done to Ensure Privacy and Security of Records?

Protecting patient data is a subject that is sure to be debated in the future due to high commercial and criminal value and the sheer volume of data available to thieves. Solving the problem of maintaining privacy, security, and accessibility for medically identifiable information will be an ongoing issue. Some novel approaches, such as smart cards developed to contain sensitive data while allowing access through communication ports and authentication control, may be the wave of the future [10].

While laws exist to provide a framework for policies and procedures, they are only as good as the people who use them. Some recommendations are discussed that may help with maintaining privacy and security in the variety of setting where medically identifiable data exists.

Hospitals

Hospitals can use a variety of tools to protect the vast number of electronic medical records it maintains. Some suggested steps are

- Controlling and recording who has access to specific identifying information while maintaining that limited access exists to portable documents, such as logs and spreadsheets [5]

- Random audits to help identify how well a facility is conforming to provider and HIPAA policies. Reviews of security activities can also be performed, such as access reports, audit logs, or security incident tracking reports [11].

- System identifications and access records: system users must abide by using their own IDs to access digital records, consistently log off when the session is finished, and never share their login information with others to ensure that unauthorized access cannot happen. User IDs can be used to detect the identity of the individual accessing the system; the time, date, and duration of the session; and the information or screens viewed; therefore, they should be carefully guarded. This information can also show if the user's access was intentional or the result of a mistake. Patients may also request who has had access to their records and that information must be provided with an audit [7].

- Sanctions or disciplinary action for not enforcing policies: policies and procedures are enacted for the purpose of safeguarding information and protecting consumers and the providers themselves. Penalties for not following rules and procedures should be enforced with disciplinary actions depending on the severity of the offense and the information accesses or compromised [7].
- Staff trained prior to implementing systems and ongoing by those with industry recognized certifications: policies and procedures should be in place to detect and promote awareness of fraudulent activity and respond with procedures that address fraud and abuse [12].
- Training in social engineering can also make staff aware of the dangers of being persuaded or manipulated to offer patient data to those who pose as health care professionals. Proper authentication of those seeking patient data cannot be overstated to prohibit releasing sensitive information the seeker is not authorized to obtain [4].
- Paper chart backups for system downtime or compromise.
- Implementing secure servers and networks to guard against intrusions, including monitoring for compromised data and disclosure.
- Maintain and enforce access policies to prohibit or limit portable access to patient identifying data.

Outside Vendors and Insurers

Business entities with ties to HIPAA-covered systems are bound by the HITECH Act and the Omnibus Rules and therefore are required to adhere to HIPAA breach notification requirements. While the vendor is onsite and requires access to a patient record, they should be logged in, authorized, and monitored by another employee. When off-site record access is needed, a fax can provide needed information while restricting sensitive personal information as well as recipients of that data. The requesting party can also be required to provide identifying credentials before medical records are released, such as each patient's social security number, before any actions are initialized [7[. Attention to employee interactions with electronic medical records needs to be a focus, as Kroll reports that employees contribute 45% of deliberate and accidental actions that lead to breaches [7].

A promising development is happening at the CMS, which is developing the Integrated Data Repository to centralize and warehouse Medicare and Medicaid claims. This process would allow data analysis to detect inaccurate or fraudulent claims before they are paid by showing patterns of behavior or trends and also providing real time pictures of claim and payment information for law enforcement purposes and detection. In addition, this data could be organized and monitored to prevent overpayments or double payments [12].

Compromised Devices

Since the majority of beaches and thefts occur on portable devices, it is reasonable to focus on discussing actions that can reduce risk to vulnerable data.

- Key management. This process refers to administratively controlling and securing encryption keys. An organization may have more than one or multiple encryption tools that require protection and organization and secure retrieval [11].
- Encryption. While encryption is a logical safeguard, it is only as safe as the entity's ability to employ a strong encryption algorithm and then keep the key to that algorithm protected [13]. Miller & Tucker discuss the effect of increased fraud in companies that use encryption. They stress that this can be attributed to a lack of otherwise prudent business practices such as broad policies and procedures, comprehensive awareness programs and manual access controls, and powerful identification protocols. They state that only employing encryption is not enough and may encourage laziness in other access controls, which can contribute to loss of data if the employees feel it is secure and do not need to take other protective measures [13].
- Remote wiping or disabling. This feature can be enabled on a device that would allow data to be remotely erased in the event of loss or theft.
- Strong password protection as well as timed logouts can aid in automatic system security [4].
- Protection at the file level. Rafalin advocates protecting data at the file level due to data access at both the cloud and mobile device level. He reasons that if the data at the file level is safe, losing or compromising the hardware ceases to be an issue as the data will not be accessible [14]. This approach could secure information on mobile devices no matter their location and enable deletion or denial of access to any file on the mobile device.
- Virtual private networks can be utilized on mobile devices by way of a web browser or a cloud provided application. This process is not without risks due to interception in transit or authenticating users at either end of the transmission [11].

Cloud Service Providers

Cloud services are an increasing factor with mobile healthcare devices and present their own challenges to availability, integrity, and confidentiality of health data. The Department of Health and Human Services Office of Civil Rights published the Omnibus Rules to amend the HIPAA rules. As discussed earlier, these rules define the business associate and subcontractor relationship and whether they are held to the HIPAA standards. Cloud providers must understand their status in relationship to these rules [11].

Business associate agreements are that which define expectations between HIPAA covered entities that trade medically identifiable information. These agreements maintain that those business associates will abide by agreed upon guidelines for data security and privacy, including breach notification and action protocols. Business associate agreements are crucial to the privacy, security, and integrity of information maintained by cloud providers as they spell out how data is accessed, used, and for how long as well as how it is disposed. It also spells out how information is collected, managed and used by the provider. Equally important, the agreement should discuss what the provider is not responsible for. This is important as risks may be involved with storing data in multiple locations or countries, thereby falling under different laws and jurisdictions that may affect privacy and security laws [11].

Cloud provider services present unique circumstances when it comes to security and privacy of medical data. A central issue is who has control of the data and how the data will be maintained. As cloud services are deployed on several platforms, varying levels of control exist and should be defined and agreed up on in the business agreement [11].

The control of information is further affected by the deployment model. Public clouds open infrastructure to the public and lose data control upon deployment. Private clouds have only one customer and are therefore much more secure. Community clouds are available to particular communities while hybrid cloud are a combination of private and public models. Private clouds are the obvious choice for medically indefinable data [11].

Shared multitenant environments are an important area of risk for the public models. These models offer cost effectiveness from sharing infrastructure and resources with other customers. Some of the risks involved with this model include the possibility that one consumer may access the information of another consumer or that information can be co-mingled. Other considerations include availability and performance issues that may exist when one consumer impedes the performance of another. Cloud service providers may not be able to separate the activity of individual consumers. These considerations affect access and availability as well as information deletion. Cloud providers must define their data separation policies, such as database and application level isolation [11].

Education

Individuals need to be educated on the importance of safeguarding their medically identifying data as well as their financially identification. They are the first line of defense in detecting and deterring compromised medical identities. The credit card industry implemented complex analytical systems to detect fraudulent activity. Notifying consumers of potential criminal activity increased awareness to identity theft and made consumers a partner in decreasing fraud within the credit card industry [8]. Gordon, 2013). Many consumers do not know how to access or monitor their health records, and even if consumers do detect medical identity theft, the chore or resolution may prove discouraging. The Ponemon Institute reports that of those survey respondents who did attempt to resolve fraudulent use of their records through their provider or insurance company, half state that is still not resolved, while a third reported the process taking a year or longer [2].

The closet method the healthcare industry has in enlisting consumers is the explanation of benefits (EOB) that is delivered when a medical procedure is performed. The EOB outlines details of services rendered, insurance information, and payment responsibilities. Insurance companies should make these statements as easy to read as possible.

Consumers typically do not pay close attention to these benefits and usually are only concerned with payment information and if they did notice a discrepancy, they would still need to take action. Much of the public is unaware of medical identity theft and its consequences, both financially and in terms of patient safety [8]. The Ponemon Institute reports that half of the medical identity theft survey respondents failed to take further steps to prevent future medical identify compromise and only a third stating they will more closely examine their explanation of benefits [2].

The Medical Identity Fraud Alliance was created to address some of the issues presented in this paper. Compromised of representatives from stakeholders across the healthcare spectrum, the Alliance is designed to develop awareness and education for both the public and healthcare sectors by developing standards and practices to detect and prevent medical identity theft through a public, private sector partnership [8].

The Affordable Care Act adds some additional safeguards for Medicare and Medicaid programs. The new policies provide

- A strict screening process for participant categories that have a pattern of fraudulent activity.
- New policy that States will have to examine service providers that refer or provide Medicaid recipients for histories of fraudulent activity. Any service provider already banned from another State's Medicare or Medicaid program will be banned from all State's Medicare and Medicaid programs.
- Using predictive software to detect patterns or areas of fraudulent activity so that enrollment in that area may be stopped or examined on a closer level.
- Stops payments on a temporary basis in cases of suspected fraudulent activity by service providers and suppliers. The new policies allow halted payment activity while an investigation is undertaken [14].

Conclusions

The initial research questions asked if current controls are effective in ensuring the privacy, integrity, and security of electronic medical information and the conclusion is definitely not. Loss and theft of mobile devices are the biggest contributor of medical breaches affecting over 500 records. While several federal laws exist to give a framework to security policies and procedures, lack of appropriate employee behavior has a direct effect on this statistic. Electronic medical record theft can lead to identity theft and medical identity theft, which can not only cost consumers and providers large sums of money, but can result in injury or death of the patient and liability issues for the providers. By focusing on mobile device security and privacy issues, many mitigations are discussed which may help to reduce the risk to patients and providers. The largest area of mitigation is education, of both the consumer and provider, on the prevalence of medical identity theft and detectable risks in the various levels of the data lifecycle.

References

1[] DataFile. (2014). It's Getting Scary Out There, in HIPAA Breach Land. Retrieved from http://www.datafiletechnologies.com/hipaa-breach-statistics-2012/#.U7n29Vbn9DA

[2] Ponemon Institute. (2013). 2013 Survey on Medical Identity Theft. *Ponemon Institute.* Retrieved from http://www.ponemon.org/blog/2013-survey-on-medical-identity-theft

[3] Department of Health and Human Services. (2012). CMS Response to Breaches and Identity Theft. Office of Inspector General. Retrieved from https://oig.hhs.gov/oei/reports/oei-02-10-00040.pdf

[4] Taitsman, J. K., Grimm, C. M., & Agrawal, S. (2013). Protecting Patient Privacy and Data Security. *The New England Journal of Medicine, 368*(11), 977-9. Retrieved from http://www.nejm.org/doi/full/10.1056/NEJMp1215258

[5] Camp, L. J., & Johnson, E. J. (2012). *The Economics of Financial and Medical Identity Theft.* Philadelphia: Springer.

[6] Kierkegaard, P. (2012, April). Medical Data Breaches: Notification Delayed Is Notification Denied. *Computer Law & Security Review*, *28*(2), 163-183.

[7] Kopala, B. (2011). Use of Digital Health Records Raises Ethics Concerns. *Jona's Healthcare* Law, *Ethics and Regulation*, *13(*3), 84-89.

[8] Gordon, G. E. (2013). The Growing Threat of Medical Identity Fraud: A Call to Action. *Medical Identity Fraud Alliance.* Retrieved from http://medidfraud.org/wp-Content/uploads/2013/07/MIFA-Growing-Threat-07232013.pdf

[9] Kroll Advisory Solutions. (2012). *2012 HIMSS Analytics Report: Security of Patient Data.* Retrieved from http://www.krollcybersecurity.com/white-papers/himss-2012-report.aspx

[10] Honnegowda, L., Chan, S. & Lau, C.T. (2013, March). Embedded Electronic Smart Card for Financial and Healthcare Information Transaction. *Journal of Advances in Computer Network*, *1*(1), 57-60.

[11] Gilmer, E. (2013, April). *Privacy and Security of Patient Data in the Cloud*. Retrieved from http://www.ibm.com/developerworks/library/cl-hipaa/

[12] Morris, L. (2009). Combating Fraud in Health Care: An Essential Component of Any Cost Containment Strategy. *Health Affairs*, *28*(5). Retrieved from http://content.healthaffairs.org/content/28/5/1351.full

[13] Miller, A. R., Tucker, C. E. (2011). Encryption and the Loss of Patient Data. *Journal of Policy Analysis and Management*, *30*(3). doi/10.1002/pam.20590/pdf.

[14] Buredetti, P. (2011, February 15). *Fighting Fraud and Waste in Medicare and Medicaid*. Department of Health and Human Services. Retrieved from http://www.hhs.gov/ asl/testify/2011/02/t20110215b.html

Biographies

SUSAN FOWLER is a graduate student in computer and information technology at Purdue University. Her interests include mobile device forensics, security and privacy in technology, and risk analysis.

SAM LILES is an associate professor at Purdue University specializing in transnational cyber threats and digital forensics incident response. His appointment is in the College of Technology in the Department of Computer Information and Technology. He has held appointments as a professor at Purdue University, Calumet, in the Computer Information Technology Department and at The National Defense University where he taught in the Department of Cyber Integration and Information Operations. He has served in the United States military, law enforcement, federal government, and has consulted to corporate information security organizations. Dr. Liles has a PhD from Purdue University, where he studied cyber conflict, and a master's degree in Computer Science from Colorado Technical University.