Examining Locking Down of Electronic Medical Records

Ryan Carr, Sudip Chakraborty, Leah Johnson, Jasmin Miravete, and Joshua Vega
Department of Computer Science, Valdosta State University, Valdosta, GA, USA

Abstract – In the rapidly changing world tools used for everyday life are changing even faster. Health care is one of the areas in our daily life that is changing so that health care professionals can coordinate better care for their patients. Hence, out of many ways, the medical field is shifting from paper records to electronic medical record (EMR) to achieve the above goal. However, the urge for digitization of health records has placed the confidentiality, integrity, and availability of personal sensitive information (health records) at risk to be compromised. In this paper, we examine the security related to EMR and the role of U.S. federal government’s push to digitization of health records. We examine HIPAA and ARRA in the context. We present examples of threats and attacks, with statistical data, related to EMR. We also discuss potential damage in a breach and, finally, examine the ways to secure it. This paper is our attempt to highlight the importance of security concerns in digitization of health records.

Keywords: Health Records, EMR, Security, Privacy, HIPAA, ARRA, Digitization

1 Introduction

A patient’s medical record is an invaluable asset to all involved entities, including health insurer and pharmacy, in health care services. It is undeniable that a prompt access to such records is of high importance, especially for physicians and health care providers. The traditional form of recording and storing these records can satisfy this demand only to a limited extent. While it still works within close proximities (within a clinic, or across two services in a short distance), it is not sufficient for exchange of, or discussion on such records over larger distances. Traditional paper format of storing health records is not conducive to exchange of it in a time-sensitive manner, especially in a collaborative environment where the physicians or health care providers are not within close proximities. Therefore, digitization of health care records becomes a natural choice. Consequently, we have observed tremendous growth in software for creation, maintenance, storage, and exchange of electronic medical records (EMRs). These alleviated issues related to storage, access, and exchange of health records in traditional format. It is also found to be time and cost effective as duplication, storage, and exchange is faster and cheaper. However, with all these benefits, EMRs bring unique challenges that are not much pertinent in traditional format of health records. The major concern that rise is who has access to it and how secure is it? These issues are of great importance as health records are very sensitive private information that should not be accessed by anyone other than a selected set of entities (physician, health care provider, insurer, and patient). In the traditional format the record is created and stored within a specific facility and can be accessed by certain entities involved in the facility only. It is also expected that the records will be stored in secure manner (under lock and key in a proper cabinet). With EMR these expectations erode as digital records are stored on computers and exchanged over the Internet. Though a standard securing mechanism can be placed, a suspicion about the sufficiency to maintain confidentiality and privacy of the records can rise. This is especially due to lack of control on the communication over the Internet. Also, enforcement of proper access control and authorization become more complex compared to the traditional format. The entities in this context must rely on the software, which are developed by entities not involved in the health care environment. The efficacy can be questioned even further if such EMRs are stored on Cloud storage that are often under the control of third parties. Hence, there is a strong need for examining privacy & security concerns related EMR, keeping track of incidents or events targeting breach of such security, designing & deployment of appropriate security measures, and creating legislation to address deterrence and violations. In the light of these objectives, especially the last one, in this paper we examine the state of securing EMRs. We explore the origin of EMRs popularity in recent times and role of legislation like ARRA, HIPAA in its growth. It is found that HITECH part of ARRA has a major role to play for increase in adoption of EMRs. We highlight security concerns and potential damage resulting from a breach of security. We present the data available to demonstrate severity of the issue. We also suggest few basic breach prevention mechanisms that can be applied to systems involving EMRs.

The rest of the article is organized as follows: Section 2 gives a detailed overview of the legislation forming ARRA and HIPAA. Section 3 identifies existing security concerns. Section 4 discusses potential damages that can be done with compromised information and provides examples of actual breaches. Section 5 proposes a variety of ways to further improve security of sensitive medical information. Finally, we conclude the work in Section 6.

2 Government Role in EMRs

The first half of the last decade observed a big surge in use of EMRs in the USA. More and more physicians started enjoying the benefits of the system. According to the Office of the National Coordinator for Health Information Technology percentage of physicians using EMR for e-prescriptions rose
from 7% to 66% in 5 years. Figure 1 illustrates county-wise distribution of percentage of physicians using EMR for above stated purpose.

![Distribution of percentage of physicians using EMR for above stated purpose.](image)

Figure 1. Percentage of participating physicians e-Prescribing through EMRs in USA [16]

## 2.1 HITECH under ARRA for EMRs

The last decade showed an economic instability whose effect was observed throughout the world including the United States. In an attempt to revitalize the economy, the U.S. Congress responded to this economic weakness by enacting a multitude of stimulus packages. The American Recovery and Reinvestment Act of 2009 (ARRA) was one such stimulus package that aimed to lessen the effects of the recession on American citizens [1], [2]. Under the ARRA, the Health Information Technology for Economic and Clinical Health Act (HITECH) made a push towards Electronic Medical Records, to cut down on government spending and health care costs. To enforce their push for EMRs, the government offered certain incentives for eligible facilities. Essentially, these incentives offered any medical facility “incentive payments”, both to physicians and to the hospitals themselves. To continue receiving these incentives, health care providers had to provide “meaningful use” of EMRs [3]. Meaningful use is defined as using electronic health records to: (i) improve quality, safety, efficiency, and reduce health disparities, (ii) improve care condition, and (iii) maintain privacy & security of health information [4].

These incentive payments were given out from 2011 to 2016, and gradually decreased every year, allowing EMR users to earn up to $44,000 dollars [5]. Another motivating factor for the switch to EMRs is the penalty incurred should a facility not comply. The penalty for any medical personal who didn’t utilize or show meaningful use of EMRs by 2015 was a 1% reduction in Medicare reimbursements received. That percentage increased 1% each year to a maximum of 5% [6]. Thus, since then, EMR use by physicians has steadily increased to over 83% [7]. Another reason for increased EMR use is due to the convenience they offer. The EMR allows patients’ medical records to move with them digitally, and it gives the health facilities an overall view of a patient’s health. Figure 1 shows just how widely used EMRs have become since ARRA was enacted to the year 2013 [14].

## 2.2 HIPAA

In 1996, Congress realized that technological advancements could make it increasingly difficult to secure the privacy of health information. Consequently, the Health Insurance Portability and Accountability Act of 1996, or HIPPA, was enacted. This piece of legislation required that the Departments of Health and Human Services (HHS) is to establish a set of national standards for electronic healthcare transactions, health identifiers, and security. The HHS published two main rules: The Privacy Rule and the Security Rule [8].

### 2.2.1 HIPAA Privacy Rule

The Privacy Rule is a nation-wide set of standards that protects all “individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media whether electronic, paper, or oral. The Privacy Rule calls this information “protected health information” (PHI). This protected information includes:

- Individual’s past, present and future physical or mental health condition.
- The provision of health care to the individual.
- The past, present, or future payment for the provision of health care to the individual [10].

Under the Privacy Rule, clients are given the right to get a copy of their medical records, have corrections made to it, receive notification about how their medical information is being used or shared, to decide whom they want their information shared with, and to get a report for why and when it was shared. Additionally, the Privacy Rule even limits who can share and receive your medical information. Medical information is only shared if it is necessary for the client’s health; it is needed for payment; the client explicitly names friends or family members who can receive it; the information is used to ensure public’s health; and it can be shared with law enforcement [9].

### 2.2.2 HIPAA Security Rule

The Security Rule provides the set of standards for ensuring the protection of confidentiality, integrity, and availability of electronic PHI. The main goal of the Security Rule is to protect the privacy of the individual while allowing the covered entity to implement the appropriate policies, technology, and procedure. Because of this, the Security Rule is designed to be flexible and scalable. The Security Rule is composed of four sub rules; all covered entities must:

1. Ensure the confidentiality, integrity, and availability of all electronic PHI they handle.
2. Identify and protect against reasonably anticipated threats to the security of PHI.
3. Protect against reasonably anticipated use or disclosures from unauthorized individuals.
2.2.2 HIPAA Overall

The Privacy Rule and Security Rule of HIPAA apply to health plans, health care clearing houses, and any health care providers who transmit health information in electronic form about transactions for which the Secretary of HHS has adopted standards under HIPAA. Due to revisions made by HITECH, even business associates are covered and are required to follow HIPAA regulation. To ensure that business associates comply, they must sign business associate agreements. Moreover, subcontractors of business associates may also be required to comply with HIPAA regulation. In addition to the previously listed PHI, HIPAA also protects information regarding an individual’s: (i) Name, (ii) Specific Dates (birth, admission, discharge, death, etc.), (iii) Phone number, (iv) Social Security Number, (v) Medical Record Numbers, (vi) Photographs, and (vii) City info, ZIP, and other geographic location identifiers. The exceptions of HIPAA apply to the people who are not required to abide by HIPAA regulations include, but are not limited to, life insurers, employers, workers’ compensation carriers, schools and school districts, certain state agencies, law enforcement, and many municipal offices [9].

3 Security Concerns

Even with HIPAA in place, there is always a level of security risk. Security breaches regarding medical information is becoming a common form security issue. Health and medical companies are becoming more lucrative targets of hackers and, as a 2014 report showed, account for nearly 43% of reported breaches [12]. According to data released by Office for Civil Rights, Dept. of Health and Human Services of USA, there is growth in number of breaches of health-related information [22]. The following figure shows the number of PHI breaches between 2009 – 2016, where each breach has affected at least 500 individuals.

Also, according to joint ONC/AHA report (September 2016), 95% of the hospitals now allow patients to access e-PHI for viewing [21]. This is four times increase over a four-year period, as shown in Figure 3.

The above increasing trends tally with information presented in Figure 1 and gives idea about the complexity & size of the problem, as EMRs have become substantially more commonly used. It becomes even more concerning when we observe that since 2013, the number people affected by breaches of their PHI via hacking and other IT methods has increased exponentially, which is depicted in Figure 4.

The above figure shows that there is a very sharp rise in number of individuals affected by security breaches of health records in 2015. While non-IT/hacking related incidents (for example, theft, loss, improper use or disposal etc.) were the major contributor to affect individuals between 2010 – 2014, hacking or IT-related incidents contributed more than 99% to the total number of individuals affected in 2015 [14]. This forced us to examine further and identify the source of the security breaches. We compared the sources of health information breaches in 2010 and with that of 2015. The pie charts in Figure 5a and 5b show the percentage of individuals affected by information breaches in different sources like desktop computers, laptops, portable devices, emails, paper documents, network servers, and other forms of breaches, in the year 2010 and 2015 respectively. In 2010 majority of the individuals
affected were related to other form breaches and by information breaches from laptop.

Figure 5a. Percentage of individuals affected by different sources of breaches in 2010

However, it is observed that in 2015 majority of the individuals (95% of who were affected in some form of health information breaches) were affected by security breaches in network servers, as evident from Figure 5b.

Figure 5b. Percentage of individuals affected by different sources of breaches in 2015

This rise in percentage of individuals affected by network related breaches can be attributed to increase in use of EMR and their storage on various networked storages (like web servers and Clouds) and exchange over public networks like the Internet. Therefore, it is of utmost importance to store the PHIs securely on the servers and use encrypted/secure channels for sharing these sensitive records.

3.1 Contributing Factors

There are several reasons why these numbers are so high. As discussed above, rise in use and exchange of e-PHI in recent years is one of the main contributors, but there are other factors that really make impacts are:

- **Lack of trained IT experts in the field of security**, especially, secure management of e-PHI,
- **Budget**: because there is a scarcity of IT experts, their salary is significantly higher; thus, healthcare facilities cannot afford to hire more,
- **Outdated Technology**: Healthcare facilities are usually behind other industries in adapting new technologies, which results in them outdated technology [12].

Level of impacts of each of the above on secure management of EMRs can be investigated separately. However, we did not include that analysis within the scope of the current article.

4 Potential for Damage

The potential for damage varies greatly when it comes to PHI breaches. The breaches can come from mainly two sources, outside attackers and insiders (individuals involved in creation and maintenance of the EMRs). First, let’s examine the potential damage that can be caused by outsiders:

4.1 Impact of Outsiders Attack

There are basically two possibilities when a hacker or cyber-attacker gains access to an individual’s medical record – either they cause loss of identity of the victim resulting in financial issues of varying degrees (small to massive), or they cause little or no damage at all. For example, if a medical care employee left their personal laptop in their vehicle, and on the laptop that individual had sensitive, unencrypted medical information in one of the folders. If someone broke into the car and stole the device the security of those files has been compromised, technically, because the criminal now has potential access to this sensitive information; however, this does not necessarily mean that the criminal will use, or can use, or even successfully access, those files on the computer. It is quite possible that the criminal was not after the data on the laptop, rather he was after the laptop itself. In such a scenario, no damage was caused through the breach of that information.

On the other hand, attackers who are intentionally after this information can use the information for identity theft, credit card theft, blackmail, and even to obtain prescription medication or services on the victim’s behalf. Following we highlight some concrete examples of breach incidents of this sort happened in the USA.

In June 2014, in Montana, hackers breached the security of EMRs that compromised approximately 1.3 million people’s Social Security Numbers and other personal information. To compensate the damage, individuals whose information may have been compromised were given free credit monitoring and identity protection insurance. These “free” services were covered by a two-million-dollar state insurance policy regarding cyber security [20]. In another incident, later in the same year, administrators at Clay County Hospital in Illinois received a notification demanding a ransom be paid to protect the PHIs. The hackers threatened to release the PHI information gathered from the hospital. The hospital notified the FBI and a formal investigation was conducted. No one was arrested and no information was released as the ransom letter had stated [18].
4.2 Example of Insiders Attack

PHI is not only susceptible to outsider attacks. Employees of a healthcare provider can also compromise sensitive information. As a concrete example, at Howard University Hospital in USA, a medical technician obtained 40 medical records and sold them for a total of $2,100. The person was found guilty of violating HIPAA, which has a maximum sentencing of 10 years in prison [19].

4.3 Role of Healthcare providers

The healthcare providers have a significant role in the context of potential damage in an EMR data breach. They are the primary target of these breaches. From the data, available from [22], Figure 6 shows nearly 78% of healthcare data breaches were targeted to healthcare providers in the year 2016, which is a rise in 7% points compared to that of 2015.

Figure 6. Major targeted entities in healthcare data breaches

This imposes greater responsibilities to healthcare providers in protecting individual’s health related information. In accordance to HIPAA, when there is a breach of patient PHI, healthcare providers are required to notify the US Department of Health and Human Services, all victims affected, and give a press release should the breach affect 500 or more people. If there is a breach that affects less than 500 people, healthcare providers are only required to include that information on an annual report to the government and to notify all affected individuals. However, in a survey of victims affected by medical identity theft, only about 25% of them were actually notified. Figure 7 shows the sources through which individuals came to know about medical identity theft related to them. This shows that the healthcare providers could not meet the expectation of notifying individuals about potential or actual breaches related to their accounts. One of the reasons for this failure could be the cost, as the average cost to correct implications caused by medical identity theft is $13,500 [18]. This lead to the conclusion that to reduce the overhead incurred due to breaches (especially medical identity theft), there is a need for stronger security mechanisms to protect electronic medical records.

Figure 7. Percentage of individuals aware of medical identity theft based on sources of information [18]

5 Ways to Mitigate Breaches

In this section, we briefly discuss the possible preventive mechanisms that can be adopted to alleviate the security breach issue of EMRs. There is no single security mechanism to achieve that, rather there are several approaches that the healthcare facilities can take to mitigate the number of security breaches and strengthen existing security and HIPAA regulations. The following is a suggestive list of approaches that include:

- Investing in well-educated and well-trained IT experts
- Periodical security risk analysis, vulnerability assessments, and testing
- Separation of data

Let us elaborate on the above approaches.

5.1 Investing in IT-experts

Many IT firms hire experts based on experience rather than education. This causes many young but talented IT professionals, like fresh graduates, to be overlooked because they have relatively less number of years of experience. Regular training seminars for current employees would also be of great benefit. This training should be directed towards staying up to date with new technology or recent security breaches, discussing topics such as: how a security breach happened and how it could have been prevented. Healthcare facilities may also benefit by building stronger relationships with employers and Universities to better train future graduates. Expanding internship and training programs to educate young professionals is another solution [12].
5.2 Periodic Security Risk Analysis & Testing

Healthcare facilities should conduct an annual HIPAA security risk analysis. This essentially checks for new vulnerabilities that may have arisen from changes made throughout the year, such as new employees, system deployments, and IT enhancements. Many breaches are caused by theft of a portable devices containing unencrypted information, as supported by Figure 5. Because of this, simply encrypting data-at-rest would cut down largely on the number of e-PHI breaches. This also includes hardware inside offices. Any data that is being stored should be encrypted so sensitive information cannot be retrieved [13]. To further strengthen e-PHI security, healthcare facilities could conduct more frequent vulnerability assessments and penetration testing to search for potential security risks and liabilities [13].

5.3 Separation of Data

Another good security procedure is keeping guest and professional data separate by using different wireless internet network access for each. If this is not done, then the potential for holes in security and breaches go up. The access keys for these networks should be changed regularly. Finally, access to sensitive data should be carefully monitored and regulated. Access should only be allowed on a need-to-know basis and in accordance with HIPAA guidelines [17].

However, none of the above approaches is alone sufficient to provide desired level of security for sensitive electronic medical records. Our observation is, a combination of variety of approaches, as appropriate, should be adopted and deployed to countermeasure the threat of security breaches of EMRs.

6 Conclusions

In this paper, we examine the issues and importance of securing electronic medical records (EMR) of individuals. We investigated the role of government legislations in the context and the security concerns. We discussed the trend in security breaches, potential sources and major targets in these breaches, and the consequences (extent of potential damages). After careful examination, we draw the following conclusions: the use of EMRs (or, EHRs) has increased in recent years, particularly due to the incentives offered to participants who can demonstrate meaningful use of it. Another factor for the rise in usage is the penalties incurred by not implementing and showing meaningful use. Finally, one of the major aspects is the convenience it provides for clients and medical professionals. U.S. Congress, anticipating a need for security of medical data, enacted HIPAA, which was further revised into its current version by the ARRA and HITECH Act.

HIPAA provides an infrastructure of security guidelines and regulations that are intended to secure an individual’s PHI. It is composed primarily of two major rules: The Privacy Rule, which protects an individual’s sensitive medical information, and the Security Rule, which protects the confidentiality, integrity, and availability of that information. Even with HIPAA in place, EMRs and EHRs are increasingly becoming a bigger target for hackers. Challenges that are making these quite susceptible to breaches include lack of IT experts involved in the healthcare domain, difficulty in hiring desired number of experts due to budget constraints, and latency in using state-of-the-art security technologies for protection of PHI. Should an individual’s medical and health records be compromised, the financial damage done can be devastating, which is why it is important to increase security by utilizing more preventative measures. Some of which are as simple as: encrypting data-at-rest, keeping professional wireless networks separate from public ones, and running frequent tests and diagnostics to check for potential security vulnerabilities.

7 References


