From spam to medical identity theft: Exploring the vulnerabilities of Electronic Medical Records

Anzu Hakone
Mentor: Ming Chow

December 15th 2015

Abstract

As more healthcare institutions utilize electronic medical record software (EMR) to store patient records, the number of healthcare data breaches is also on the rise. In addition to the obvious threat to privacy, there are malicious ramifications to medical information cyber attacks, with medical records valued higher on the black market than credit card or Social Security Numbers (SSN). The stolen records can be used for spamming, identify fraud, prescription and service theft, billing fraud, and in its worst case, lead to death. While electronic medical record software companies need to improve their system security, the users of the software are also at fault as this vulnerability is exacerbated by the lack of training and awareness from both the hospital employees and patients. This paper will explore the causes and ramifications of healthcare information breaches as well as suggest some possible defense tactics to prevent medical information cyber attacks.

1. Introduction

Every year, more healthcare providers are switching over to electronic medical records (EMR), also known as electronic health records (EHR), for managing patient data. EMRs serve as fast, compact methods of storing and transferring patient information as well as provide improved diagnoses using machine learning algorithms from the collected medical big data. In 2009, as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act, the federal government even began offering monetary incentive for healthcare providers to convert to EMRs [4]. Despite the many advantages, the high value of medical information on the black market and the increase in EMR use has attracted information crackers to gain illegal access to EMRs.

According to the 2014 Breach Level Index annual report, of the 1,023,108,267 total data records compromised across industry in 2014, healthcare organizations had 29,384,567 data records stolen, or 3% of the total [2]. Although 3% is still not as bad as the 55% in retail, 20% in financial, or 9% in technology industries [2], the attacks have caused the number of medical identity theft (MIT) victims to rise from 1.4 million in 2009 to over 2.3 million in 2014 [8]. This, unfortunately, is not surprising since 94% of the $3 trillion US healthcare industry [6] has suffered from cyber attacks as stated in 2014 SANS Institute report [11].

One such case included TRICARE, an organization that provides healthcare for active and retired military personnel and their dependents. In 2011, unencrypted backup tapes that contained the names, Social Security Numbers (SSNs), addresses, clinical notes, and lab test results of approximately 5 million patients were stolen from a parked car of a TRICARE

employee [12]. The incident was clearly a violation of the Health Insurance Portability and Accountability Act (HIPAA), which protects the privacy of health information (PHI) and personally identifiable information (PII) of individuals [4]. The TRICARE victims suffered from identity theft and MIT, which is defined as "fraudulent theft of an individual's PHI and PII…to obtain medical goods and services or for financial benefit" [4].

EMR systems can be either locally-housed at the hospital, such as Epic and Centricity, or web-based, such as eClinicalWorks, McKesson, and Cerner [1]. The two types of EMRs have different security vulnerabilities and thus defenses, but the cost of EMR system breach is the same – invasion of privacy and criminal activities including identity theft. Because every individual will seek medical attention at some point in their lives, medical information theft is an issue that needs to be addressed and acknowledged by everyone, not just those in the cyber security field.

2. To the Community

2.1 What is the cost of medical record?

According to the Ponemon Institute, a security and privacy research organization, damage from MIT costs approximately $11.6 billion per year [4]. Although two-thirds of medical data breaches did not result in financial damages, the remaining third each paid approximately $18,000 to restore their information [11]. This is because unlike credit card numbers, which can be cancelled upon detecting fraudulent use, stolen medical information requires additional cost of correcting inaccuracies in their health records, reimbursing healthcare providers, restoring credit, amongst others [8].

In its worst case, stolen medical information could result in death. The Medical Identity Fraud Alliance (MIFA) reported an incident in which an elderly man was taken to the emergency room for a back injury [4]. Despite his life-threatening allergy to penicillin, he was administered the drug because his medical records did not indicate such allergy. This occurred because the victim had lost his medical ID card, and the thief had used it to receive medical services including one using penicillin. Like so, EMR theft could create inaccuracies in the victim's medical records of which could have severe consequences.

Not only are medical information more difficult to restore than credit cards or SSNs, but they are also more valuable to crackers. Whereas credit card numbers and SSNs are worth only a couple of dollars on the black market, medical information are sold as high as $50 [4]. So why are EMRs more valuable? EMRs include a wide range of information about an individual, and thus crackers can exploit in various domains from just one entry of an EMR. Figure 1 shows the types of information associated in an EMR and their corresponding illicit uses.

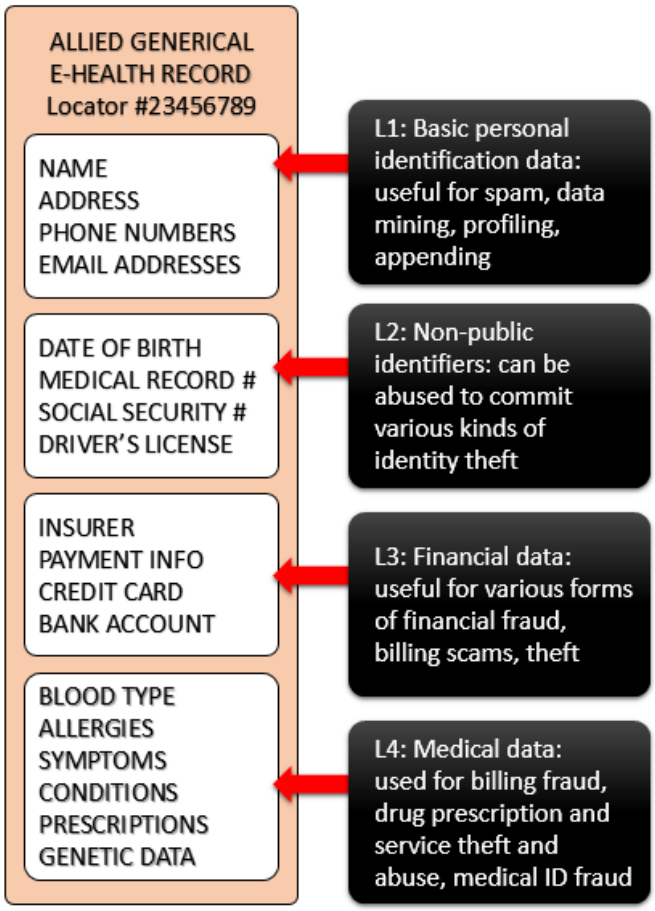

Figure 1. Sample EMR and possible illicit uses [3].

Level one includes information that are accessible without hacking knowledge but can still be valuable on the black market since it can be used to spam "fresh targets" [3]. Level two information can be used for identity theft, creating fake IDs, opening credit card accounts, committing tax fraud, and answering challenge questions to online accounts. Level three provides additional information for making fraudulent activities mentioned in level two easier. Finally, although the buyer pool is smaller because it involves specific information, data in level four can be very valuable. It can be sold to individuals who have similar donor records and desire medical procedures and services that may be difficult to receive otherwise, or to commit

healthcare fraud like the Affordable Care Act (ACA) fraud [4]. It can also be used to create fake medical IDs to buy medical equipment or prescriptions that can be used by the black market buyer themselves or be resold for profit [6]. Like Rick Kam, the president of ID Experts, said, healthcare data "is like a box of chocolates" [8].

2.2 Why are there so much medical data leaked?

In order to defend against crackers, we must first identify and understand the causes of these EMR breaches. Because EMRs can be both locally-housed or web-based, there are both system and human vulnerabilities that contribute to medical data leaks.

2.2.1 System vulnerabilities of EMRs

Vulnerabilities in software is common and often unavoidable, but an important factor in addressing these vulnerabilities is the presence of proper bug reporting systems to publicize findings and improve the community [9]. Of the 83 EMRs reviewed in a security report, many of which were rated as top EMR software, none had an official security vulnerability reporting system [9]. In fact, emails to the reporting admin were undeliverable for 55 out of the 83 EMRs. For the EMRs with emails that did go through to the reporting system, the response rate was less than 10%, and they either reported that their systems were not vulnerable or only confirmed that they received the report – only one EMR software confirmed the vulnerability and that they were working on a solution.

As mobile devices become more convenient and widespread, EMRs are beginning to be available on portable devices such as Personal Digital Assistants (PDA), tablets, and flash

memory cards [10]. However, security on these portable devices are not yet comparable to to computer systems, and between 2009 and 2011, mobile devices were responsible for of exposing information of 1.9 million patients. Crackers can exploit unsecure phones and auto-login capabilities of mobile apps to obtain passwords and credentials [4]. Once the criminal has access to the EMR system, they can read data, and modify or execute code that will expose data when doctors and patients log onto the system.

2.2.2 Uninformed patients

Most patients are uninformed and unaware of the sources and consequences of medical data theft. Thus, patients often discover stolen medical IDs *after* they have been used to illicitly obtain medical procedures or services [6]. Many of the MIT and fraud were committed by those the victim knows, such as relatives of the victims (35% of cases) or medical providers billing for undelivered services (29% of cases) [4].

Scammers and crackers often exploit the patients' lack of knowledge of fraudulent tactics to gain personal information. For example, a 69-year-old man used an online tool to sign up for healthcare [4]. Shortly after doing so, he started receiving emails and calls from an individual who claimed to be from the national Medicare and Medicaid office. The individual said that Medicare will send his new Medicare card as soon as they receive his bank account number to confirm his identity. Unfortunately, these were acts of phishing and spam, and if the victim is unaware of these scamming methods, they may expose their medical and financial information to criminals.

2.2.3 Healthcare personnel

As was with the TRICARE case, one of the vulnerabilities of EMRs are the employees of EMR companies and hospitals. According to the Ponemon report, 96% of healthcare organizations experienced theft of or misplaced physical devices, many due to employee negligence [8]. Millions of medical information could be stolen by simply breaking into an office or vehicle and stealing a computer, or even accessing an unattended computer in a hospital [10].

In some instances, the hospital personnel themselves are the criminals. Outsourcing business associates, suppliers, vendors, and partners have become popular in healthcare, but screenings and assessments of these third-party individuals have been lacking [10]. Laurie Napper, a medical technician at Howard University Hospital, used her position to gain access and sell patient medical information [12]. It was not until 17-months later that the breach was detected, and during that time, the buyer used the medical data to order prescriptions illicitly.

2.2.4 Hospital IT structure

The biggest contributing factor to EMR vulnerabilities is the way in which EMRs are used and setup in hospitals. Because cyber security is often an afterthought in healthcare organizations, hospitals often do not have the most cutting edge computer systems or cyber analysts to defend against attackers [6]. Jeff Horne, the VP of a cyber security firm Accuvant, said that most hospitals are using computer systems that are over ten years old and do not have the latest security features. In addition, some firewalls and antivirus programs may be accidentally turned off during system upgrades, allowing crackers easy access to the EMRs [5]. Old systems could also be using insecure data transfer methods like FTP when passing around health information

between business partners, service providers, and customers, leaving the transferred data vulnerable to cyber attacks [10].

Although physical theft is not a problem for web-based EMRs, EMRs that utilize cloud computing suffers from the additional security vulnerabilities of using the cloud [10]. By having to use the internet to access the EMR system, hospital computers and mobile devices are exposed to viruses and worms that could infiltrate the hospital network and affect both the EMR system and other medical devices (e.g., drug administering pumps) [5].

Hospitals are also lacking in assessments and reports post security breaches. Although required by the HIPAA, only 50% of hospitals had the four-factor risk assessment procedure in place after cyber attacks [8]. The four factors that assess the severity of the breach include: 1. amount of PHI involved in the breach, 2. persons involved in the breach (i.e., crackers and buyers), 3. if any PHI was actually accessed, and 4. what has been done to defend against the attack. As mentioned in the system vulnerabilities of EMRs, proper reporting structures and procedures are vital in improving security, and without them, crackers may exploit the same vulnerabilities to attack EMRs.

3. Defenses

As with other IT systems, it is highly unlikely to perfect EMR software to be immune to cyber attacks. However, there are changes that the US government, EMR companies, patients, and hospitals can make in order to mitigate the number of EMR breaches.

3.1 Law

With the HIPAA of 2009, hospitals must now notify both the Department of Health and Human Services and the media when there is a cyber attack that affects 500 or more patients [12]. However, there are not yet laws that require criminal prosecution [6]. The US government should enact stricter laws that help protect medical information of individuals. Currently, 65% of healthcare organizations do not offer recovery services for victims of MIT [8]. One way to encourage EMR companies and hospitals to invest in healthcare cyber security might be to impose large fines for when patients' data are compromised [12].

3.2 EMR companies

One of the vulnerabilities of EMR software was the lack of a proper vulnerability reporting system. EMR companies should implement a well-established bug reporting mechanism such as Bug Bounty of GitHub or Whitehat of Facebook [9]. This mechanism should include a responsive email address in the form of security@{vendor-domain} (standard in Open Web Application Security Project guideline) or to a private contact. Additionally, if the EMR software is available on mobile devices, security should be improved such as limiting application use if secure connections cannot be established.

3.3 Patients

Patients do not have to idly fall victim to MITs; there are measures to prevent and detect when one's medical information has been stolen or compromised.

3.3.1 Prevention

Create strong passwords and change them often [7]. Not all passwords are created equal – although all passwords can be cracked using brute force, more complicated passwords take much longer to crack than simple, weak passwords. Strong passwords: are non-dictionary words or names; contains an upper case, lower case, numbers, and symbols; are different from previous passwords; are more than eight characters long; and do not contain any personal identifiers such as birthdays.

Store documents in a secure location (physically and digitally) and dispose of them properly [7]. Physical copies of documents should be in a safety box, and digital data should be encrypted, on a password-protected computer. Old medical records and prescription labels should be shredded, and hard drives should be secure wiped when reselling old devices.

Get informed about how and where personal information is shared [7]. The chances of MIT increases as more parties have access to medical information. Patients are entitled to healthcare provider reports detailing where their information is disseminated. When in a hospital and filling out various forms, be aware and tell hospital personnel of any unattended computers and documents [7]. As said before, because 35% of MITs are committed by relatives [4], do not allow family members to use insurance or medical IDs that are not their own. Although they may not have malicious intent, this could lead to inaccurate information in medical records, which could cause misdiagnosis or unsuitable treatments.

Beware of spamming techniques [7]. Spammers often gain personal information by offering

"free" healthcare services. They may call or send phishing emails claiming to be healthcare providers or insurance companies and ask for the patient's personal information for healthcare application or "identity confirmation." Legitimate organizations will not ask for personal information over insecure channels.

3.3.2 Detection

Set up fraud alerts and credit monitoring services [7]. As with credit cards, SSN, and bank accounts, monitoring bills for unusual activity and unsolicited services [4]. Report immediately to healthcare providers and the police if a breach is detected and request them to perform a security review on their systems. Additionally, ask the involved healthcare organizations for both credit monitoring service and fraudulent activity alerts [7]. Although there is no guarantee that patient information will not be used for MIT upon a EMR breach, early detection can mitigate damages caused by MITs.

3.4 Hospitals

Hospitals personnel and IT structure are one of the biggest vulnerabilities to EMR breaches, but steps can be taken to fight those vulnerabilities. Hospitals must recognize the importance of securing their EMR systems not just because of the privacy of patients, but also since it is "cheaper to deploy safeguards than to suffer a breach," according to Deven McGraw, the director of the health privacy project at the Center for Democracy and Technology [12]. Safeguards include security patches to internet application connected to the EMR [5], firewalls and antivirus programs, data loss prevention software, device fingerprinting and reputation analysis [4],

malware detection, IP address monitoring, using cloud storage (although this may cause added vulnerability from the cloud) [12], password protection algorithms, and encryption.

In terms of IT network setup in hospitals, it is best to keep the EMR on a segregated network as to not expose other medical devices to crackers or put EMR at risk of being infiltrated by viruses and worms from mobile devices [5]. There should be a designated IT team that is solely responsible for securing the hospital network and systems and only they should have root access – EMRs and other medical software should not run on superuser rights. If a cracker gains access to medical software with root access, it becomes much easier for the cracker to control other software within the hospital network.

4. Conclusion

With the shift in utilizing technology and the environmentalists' push towards going paper-less, the day where all patient data is stored in EMRs does not seem too far. However, if the state of EMRs does not improve in terms of cyber security, many, if not, most individuals will be susceptible to identity theft and fraud. Currently, there are too many vulnerabilities from the EMR software and its users for EMRs to be a truly reliable and efficient method of managing hospital procedures and data. This is not because EMR software are inherently more difficult to secure – medical data breach is such a big problem because of the health industry's tendency to consider cyber security as an afterthought, behind the health of the patients. Although the health of patients is clearly important, MITs can also wreak havoc on the patients' lives. Hopefully the vulnerabilities and defenses mentioned in this paper will help motivate the healthcare community

to acknowledge their security problem and implement protection against medical information theft.

References

1. Anonymous. (2009, January 19). Vulnerabilities of EMR systems. *Practice Fusion*. Retrieved from http://www.practicefusion.com/blog/vulnerabilities-of-emr-systems/
2. Breach Level Index. (2014). 2014 year of mega breaches & identity theft. Retrieved from http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf
3. Camp, C. (2015, February 13). Electronic health records and data abuse: it's about more than medical info. *We Live Security*. Retrieved from http://www.welivesecurity.com/2015/02/13/medical-data-theft-fraud-ehr/
4. D'Alfonso, S. (2015, February 3). The growing problem of medial identity theft. *Security Intelligence*. Retrieved from https://securityintelligence.com/the-growing-problem-of-medical-identity-theft/
5. Hirsch, M. D. (2012, May 31). Fierce exclusive: 10 steps for thwarting HER hackers. *Fierce EMR*. Retrieved from http://www.fierceemr.com/story/fierce-exclusive-yes-you-can-thwart-hackers/2012-05-31
6. Humer, C. (2014, September 24). Your medical record is worth more to hackers than your credit card. *Reuters*. Retrieved from http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924
7. ID Experts. (2014, October 27). ID Experts releases top 10 medical identity fraud protection tips. *ID Experts*. Retrieved from

https://www2.idexpertscorp.com/blog/single/id-experts-releases-top-10-medical-identity-fraud-protection-tips

8. Kam, R. (2015, June 4). Healthcare data security is like a box of chocolates. *Healthcare IT News.* Retrieved from http://www.healthcareitnews.com/blog/healthcare-data-security-box-chocolates
9. Mandel, J. (2014, April 7). Disturbing state of EHR security vulnerability reporting. *Smart*. Retrieved from http://smarthealthit.org/2014/04/ehr-security-vulnerability-reporting/
10. McNickle, M. (2012, August 9). 5 security vulnerabilities that could mean trouble. *Healthcare IT News*. Retrieved from http://www.healthcareitnews.com/news/5-security-vulnerabilities-could-mean-trouble
11. Radcliffe, S. (2015, January 7). Patients beware: hackers are targeting your medical information. *Healthline*. Retrieved from http://www.healthline.com/health-news/hackers-are-targeting-your-medical-information-010715#4
12. Schultz, D. (2012, June 3). As patients' records go digital, theft and hacking problems grow. *Kaiser Health News*. Retrieved from http://khn.org/news/electronic-health-records-theft-hacking/