Compromises in Healthcare Privacy due to Data Breaches

S. Srinivasan, PhD
Distinguished Professor of Information Systems
Jesse H. Jones School of Business
Texas Southern University, Houston, Texas, USA

Abstract

Healthcare privacy is essential for people because any leaked information could be used against the interests of the person in providing healthcare. This is especially true in countries where the individual is responsible for getting the health insurance. In places where the healthcare coverage is included as national policy, such leaked information could be used to deny care. Healthcare industry is highly data intensive and people would need healthcare coverage in places beyond their home base. Making healthcare data available to service providers facilitates rendering quality care. This necessitates centralized storage of such data for easy access. Hackers are motivated to seek out centralized data stores due to the volume of data that they could get. Leaked data could be used by unscrupulous individuals to offer treatments that might help the people. Since such individuals are desperate to get treatment they fall victim to such scams. In this paper we first analyze some of the major data breaches in healthcare globally. We include at least one country from all the continents to see how the policies and protections for health data differs. Then we present technology-based solutions to prevent such breaches. We conclude the paper with several policy guidelines to show how the holders of health data could provide adequate data protection to prevent data breaches. This has become all the more essential because the most often breached sites are in healthcare and stolen data are used to pry on unsuspecting and vulnerable people.

Keywords: Healthcare, Privacy, Data Breaches, Policy, Security

Introduction

Organizations tend to centralize their data storage for maintaining control, manage data integrity and protect data. In many cases data protection from unauthorized access is a compliance requirement because of national law. In USA, the Health Insurance Portability and Accountability

Act (HIPAA) was enacted in 1996. It was further enhanced in 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act. These two Acts together require all healthcare providers to assure confidentiality of health data and take adequate measures to ensure security of such data. Similar laws have been enacted in United Kingdom (Data Protection Act), Europe (EU Directive 95/46/EC), Canada (Personal Information Protection and Electronic Documents Act) and Australia (Privacy Act). In spite of these Acts, there have been numerous data breaches at healthcare institutions around the world. Hackers target the health data because it does not get the same high level of protection that is afforded the financial sector data. With centralization, hackers are tempted to target the ones that are easy to tap and gather large volumes of data. The frequency and amount of data loss has created the feeling among the general public that occurrence of data breaches is the new norm in the industry.

Typically in a healthcare setting there are several different groups that are responsible for generating health data for their patients. In a hospital the patient data is gathered, the laboratories generate data from the many tests that are performed, the pharmacy is responsible for keeping up with the medical prescriptions for the patients and the distribution of drugs. In countries where a third party insurance provider is involved, there is one more source of data coming from the insurers. These subunits that generate data are not usually well integrated. This problem is typically referred to as "islands of data". This problem has persisted for many years. With the great advances in Information Technology, today it is possible to integrate all these sources of data. Protecting such hyperlinked data is essential as otherwise too much personal health information about a patient will be released without the knowledge and consent of the individual. The great risk posed by such unauthorized disclosure is that once a person's health data is released by whatever means, it cannot be retaken. In some instances the care givers may not provide the individual with the same level of dedication and care once their health data is disclosed to the wrong individuals.

In this paper we look at the practices in several countries around the world with regard to the healthcare data protection. One of the drawbacks of unauthorized release of health data is that some unscrupulous individuals might target the unsuspecting and vulnerable people with offer of help for their maladies. It is human tendency to react positively for such possibilities and get disappointed when such bad actors abuse the information that they accessed illegally. We offer guidelines to protecting health data from data breaches.

Data Breaches and Tactics Used

Data breaches have become very frequent and millions of records have been exposed. The types of data disclosed include name, address, phone number, email address, password, credit card data, health history, treatment locations, medications used, etc. Some of these data are classified as Personally Identifiable Information (PII), Personal Health Information (PHI) and Payment Card Industry (PCI) data. Organizations that collect any of these types of information have a greater need to protect PII, PHI and PCI data. Failure to do so will result in significant financial penalties. However, the existing laws have not curtailed the data breaches in the healthcare sector. In fact, one of the most breached sectors is the healthcare sector. The 2015 Data Breach Report by Verizon lists the following in order of significance (Verizon Healthcare Data Breach Report, 2015):

Healthcare	7. Entertainment
Education	8. Professional
Public sector	9. Manufacturing
Hospitality	10. Technology
Financial services	11. Administrative
Retail	12. Transportation

This report covered 25 countries and reported 1931 incidents involving 392 million records. Moreover, this report points out that PHI data breaches stand out from other breaches in that the percentage of incidents that were insider threats is equal to external threats to the businesses. Healthcare organizations should treat the data breaches in the healthcare sector as a significant threat because such web attacks are on the rise.

In this section we highlight five major data breaches in the healthcare sector or related action from around the world. The most recent major data breach in USA occurred at Anthem, a very large health insurer. This attack that happened in February 2015. It resulted in PII data being stolen for 78.8 million customers. However, no medical or financial data was stolen in this hack. Since PII data could be used for identity theft, the impact of this data breach is enormous. Also, hackers use the stolen data to commit financial fraud. It is also used in some instances to perpetrate hoaxes on the vulnerable individuals because are very conscious of their health. Unlike stolen credit card data where the stolen card can be deactivated and replaced, stolen health data cannot be withdrawn. The information contained in the health data is permanent. In 2014, the Community Health Systems was attacked by hackers from overseas. It resulted in the unauthorized disclosure of information about 4.5 million customers. Community Health Systems operate 207 hospitals in 29 of the states in USA. Thus, the impact of this breach is quite widespread. Another data breach that occurred in 2014 was in England. The National Health Service (NHS) in United Kingdom reported that data breach incidents

in healthcare doubled in 2014 from 2013. In 2013, there were a total of 91 data breaches reported and in 2014 it jumped to 183 incidents. Financial loss due to data breaches exceed $10 million in UK. Europe had over 30 major data breaches that resulted in over 300 million health records compromised. These breaches ranged from losing hardware such as a USB key or printed copies of patient information to uploading sensitive information to unauthorized websites.

In 2012, the state of Utah in USA suffered one of the easily preventable data breaches in its Medicaid database that contained data for nearly 750,000 people. In this breach, the state used a computer server that had the original default password for the hardware. Hackers who tried the default password succeeded and went on to steal health data of Medicaid patients. The government spent over $9 million to remedy the situation. In Europe and Australia, the concern presently seems to be over the breach notification requirements. Unlike USA, in Europe and Australia there are no strict notification requirements when a breach occurs. The primary reason for the push towards legislation to require customer notification is because it would spur the data holders to take greater precautions to prevent data breaches in the first place. The goal of the notifications is to protect the customer privacy (Howard, 2014). In the case of USA, the notification requirements are legislated at the state level. Out of the 50 states, 47 states have enacted varying levels of requirements for notification.

Many of the healthcare data breaches occurred due to theft of laptops or data loss, not hack by criminals. According to the California Attorney General Report, 70% of healthcare data breaches occurred due to loss or theft of laptops (Attorney General, 2012). This trend is quite prevalent in many of the healthcare data breaches because the data keepers do not provide adequate protection because of cost. Majority of the healthcare institutions in USA operate as non-profit and so they are constrained for funds. In other countries where nationalized healthcare is the norm, funding is constrained because of taxpayer support of healthcare. Consequently the major reason for frequent breaches of data in healthcare industry is attributable to lack of financial resources.

USA government and many private entities spend an enormous amount of money on healthcare. Also, they are repositories of information that are not highly protected. Consequently hackers target such institutions for attack. Moreover, monetarily health care records are more valuable to hackers than credit card data according to a report by the US Federal Bureau of Investigation (FBI). In US, the HITECH Act requires that any data breach involving 500 or more people at a healthcare facility must be posted by the Department of Health and Human Services in the Wall of Shame portal (Wall of Shame, 2015).

Best Practices to Protect Healthcare Data

Often data breaches occur due to lax enforcement of policies. Regulators in US and UK have realized the importance of security measures needed to safeguard patient data. An analysis of the various breaches shows that in some cases the patient data was sent erroneously to third parties outside the organization by mistake. In other cases it was noted that employees handling critical healthcare data did not receive adequate training in protecting such data. These are aspects that could be addressed by enforcing the organizational policies to safeguard data. However, a new trend has emerged as the cause for data loss. These are not strict data breaches, but nevertheless confidential health data was leaked intentionally by employees. Since this comes under the case of insider access to data, normal access controls would not be sufficient to prevent data leakage. The case in point is that an insider with legitimate credentials accesses the data and intentionally shares it with former employees who are disgruntled. When the employees access the health data they are within the scope of their employment and not violate the Health Insurance Portability and Accountability Act (HIPAA). However, when they send data outside the organization then they violate HIPAA requirements. To prevent such occurrences of data leakage the organization should undertake behavioral analysis for all its employees with access to sensitive information. In order to enforce this aspect of preventing data leakage by insiders, organizations should do compliance-based auditing and start using behavioral analytics. People causing breach stay within parameters of access but their pattern of access will be different from the need they have for work. One such insider access in East Texas resulted in data leakage in 2015. In US, the HIPAA was strengthened in 2009 by the HITECH Act which held the Business Associates of a healthcare provider to the same standard as the HIPAA Covered Entities in protecting patient data. Because of this requirement Cignet Health was fined $4.3 million for HIPAA violation.

Preventing data breaches should be the goal of healthcare organizations. In order to accomplish this the employees must be trained. In US, all employees of healthcare organizations are required to be trained and HIPAA compliant. However, 29% of healthcare employees did not receive any training as required. In UK which has a similar requirement under their DPA, 48% did not receive any security training. Another best practice is to do background checks on employees entrusted with access to sensitive health data. In reality this is not adhered to strictly. In US, percentage of healthcare employees receiving background checks is 60% and in UK it is 49%. This shows the need to enforce this policy in order to protect health data.

Another recommended best practice is log monitoring. Attackers often use the same IP addresses and domain names to attack multiple targets.

So, priority processing of logs will enable the businesses to monitor and know the malicious IPs. In order for this to be possible, the businesses should be willing to share data pertaining to a breach and the way the business handled the attack. This is usually available through the Incident Report but many organizations do not make available such a report. Logging all access is critical for detecting intrusion. However, logs could generate 5000 entries per second since several equipment are programmed to access the system. Because of the abundance of data being generated rapidly, it is difficult to monitor all logs manually. There should be plenty of automation in log processing and alert generation. Integration of security controls will provide a single source to monitor for discrepancies. Typically networks are color coded based on the type of data that they handle. A red network suggests lower security monitoring and black network suggests higher security monitoring. Financial systems which contain PII, PHI and PCI all reside in the black network. Usually a jump server is used to connect the red and black networks.

Threat intelligence monitoring will help healthcare institutions to be proactive. Third party threat intelligence monitoring from FireEye or similar service will help the healthcare organizations to use their resources better and implement security controls (FireEye, 2015). Compared to other businesses, healthcare organizations tend to have fewer IT security resources. Creating a strong BYOD (Bring Your Own Device) policy is essential now because many employees tend to use their devices like cell phones more at work. Use of bidirectional authentication will help in this regard. Organizational policies should prohibit storage of data locally in devices such as laptops and flash drives. Such devices are the ones lost or stolen most often and this practice facilitates data loss, not just data compromise. Businesses should have cloud storage policies as well as data backup and recovery exercises.

Often data breaches occur because an unauthorized person gained access to sensitive health data. In order to protect such data healthcare organizations should employ Identity and Access Management. This requires that access be granted only to employees with the need to perform their job duties. Using security and usage policies is a better way to control data access. The use of usage policies will help with privileged user access to data. Enforcing automatic logoff from a health source when such data user is inactive even for two minutes is essential. To prevent annoying legitimate users such logoff should be preceded by a warning. When the device is inactive even for one minute, it should force the screen display to disappear in order to protect the privacy of healthcare data. Using centralized exchanges to share health data prevents the need to actually transmit the data. Often such data transfers are vulnerable from being grabbed in transit

and sometimes such data are sent to the wrong person by mistake. Another way to protect health data is by isolating such data from the rest. This is done by creating subnets from a larger network so that there is segmentation of data. As mentioned earlier, healthcare organizations should use subnets for their patient portal, hospital record of patient data, laboratory data, pharmacy data and where relevant, health insurer data. Once again, centralized data storage gives the ability for authorized users to access all the relevant data.

One of the reasons for a successful attack over the web occurs due to users using plaintext database credentials in various web application configuration files to log into the database management system. In healthcare systems, updating the operating system to provide protection is not easy because many of the applications used by healthcare systems will not function in new operating system environment. Also, in US medical equipment are certified by the Food and Drug Administration (FDA) for use with an operating system. When the operating system is updated it is not easy to get the new certifications from FDA for old equipment. Healthcare organizations lack the resources to modify the applications with any new operating system.

Conclusion

Data breaches have become too common in general and in the healthcare sector it has become too frequent. Millions of customer records have been compromised due to insider threats, loss of portable devices with confidential data and lack of policy enforcement. This problem is not limited to any one country as explained in the details of attacks. The privacy expectations are different among countries and so the service providers should be prepared to modify their procedures to the legal requirements in the various jurisdictions that they do business. Developing adequate security policies and enforcing them is highlighted in the paper.

References:

American Bar Association. http://www.americanbar.org/content/dam/aba/publications/books/healthcare_data_breaches.authcheckdam.pdf Accessed Nov. 25, 2015

Attorney General. 2012, Data Breach Report, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf Accessed Dec. 15, 2015

FireEye. 2015. http://www.fireeye.com Accessed Dec. 15, 2015

Howard, P. N. 2014. Data Breaches in Europe. http://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/article/663/databreachesineurope.pdf Accessed Nov. 27, 2015

Privacy Rights Clearing House, 2015. https://www.privacyrightsclearinghouse.org Accessed Nov. 25, 2015

Ponemon Institute Study, 2012. Third Annual Benchmark Study on Patient Privacy and Data Security, http://www.ponemon.org Accessed Nov. 25, 2015

Verizon Healthcare Data Breach Report, 2015. http://news.verizonenterprise.com/2015/11/protected-health-information-report-preview/ Accessed 12/15/2015

Wall of Shame, 2015 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf Accessed Nov. 25, 2015