Legal issues in delivering healthcare IT solutions

Archana Indran,
H&R Block, Kansas City

Sam Ramanujan
University of Central Missouri

Someswar Kesh,
University of Central Missouri

Abstract

The healthcare industry, in an effort to provide better care, has evolved from managing patient data in heaps of files and physical records, to maintaining a single electronic medical record accessible from many platforms, devices, and locations. Users now have the ability to access data from a wide variety of portable devices like smart phones, tablets, and smart watches. This has opened up a plethora of opportunities for ease of access to personal health care data. Given the sensitive nature of such data, it has also created a wide variety of security and privacy concerns. Various laws have been enacted to protect sensitive patient information, and there are calls for even greater legal protection. While healthcare adopts the technological advancements related to mobility and other developments in information technology, it has to be careful not to violate regulations related to sensitive patient information. This may lead to fines, lawsuits, incarceration of officials, and severely damage the reputation of the health care provider.

Keywords: healthcare IT, legal healthcare, HIPAA, patient data, data security, EMR, EHR

Copyright statement: Authors retain the copyright to the manuscripts published in AABRI journals. Please see the AABRI Copyright Policy at http://www.aabri.com/copyright.html

INTRODUCTION

Innovations in information technology (IT) in the last few decades have caused a paradigm shift in the way many industries work. It has impacted their quality of work, productivity and largely reduced operating costs. The healthcare industry in particular has various advantages in adopting the advances of the IT industry; converting patient data and patient care data from paper formats to electronic format and enabling remote patient monitoring via the internet using sophisticated IT tools are examples of how this technology is leveraged to provide quality patient experience in healthcare. A major cause of concern however to make this shift soon enough, is the nature of information stored in the healthcare systems. Healthcare systems are extremely vulnerable to cyber-attacks due to the nature of the sensitive information stored in them, including an individual's medical history, insurance information and in turn even protected information such as a person's SSN, payment transactions and bank details. Access to such private information can result in identity thefts and possibly even larger crimes.

Electronic storage makes it convenient to share and distribute patient information amongst the various stakeholders. This is a potential benefit for the healthcare industry where healthcare records can be easily shared amongst physicians as well as insurance companies that need to be in the loop regarding ongoing treatments. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was the first national health privacy law introduced to regulate how health care providers, employers or insurers collect and share health information, both within and outside the healthcare system along with granting people the right to access their health information (U.S. Department of Health & Human Services, 2013).

The Health Information Technology for Economic and Clinical Health (HITECH) Act was later passed in 2009 to extend the Privacy and Security Rules of HIPAA and to promote the adoption of accurate use of health information technology. It also aimed at providing Medicare and Medicaid incentives for hospitals and physicians to take on the use of electronic health records (EHRs) and providing grants for the development of health information exchange (HIE) (HITECH Act Enforcement Interim Final Rule, 2013).

In this paper, we shall see how technology has influenced the collection, maintenance and use of electronically stored health care data. First we provide a brief description of EMR and EHR along with a discussion HIPAA and HITECH laws that are meant to regulate health related data collection and distribution. This is followed by a discussion of how IT organizations currently handle such sensitive patient information. In particular, we look into different IT technologies such as storage devices, mobile apps, cloud computing and big data, and IT practices such as outsourcing healthcare IT work that are in use for storage and distribution of health data. We also discuss the threats they encompass and how companies are dealing with this complexity. Finally, we shall conclude with the best practices and suggestions for healthcare IT industry to follow for providing security of health information and in successfully adopting to this transformation.

HEALTH INFORMATION TECHNOLOGY

Health Information Technology (or health IT) has gained importance in the last couple of decades because the advances in IT can solve some of the fragmentation inherent in health care technology. With numerous hospitals, physicians, insurance providers, laboratories and other service providers involved in handling and transferring sensitive patient data, the role of IT in

this process only made the collaborations faster and more efficient, making it possible for health care providers to better manage patient care through secure use and sharing of data. Health IT comprises of the use of electronic health records (EHRs) instead of paper medical records to maintain patients' health information (healthIT.gov, 2013).

A. EMR and HER

The National Alliance for Health Information technology (NAHIT) defines Electronic Medical Record (EMR) as:
"The electronic record of health-related information on an individual that is created, gathered, managed, and consulted by licensed clinicians and staff from a single organization who are involved in the individual's health and care." (Neal, 2008)

An EMR is an application environment created and owned by a particular hospital or care giving organization for use by their healthcare practitioners to document, monitor, and manage health care delivery within a care delivery organization. These systems are developed by individual IT vendors and sold to different hospitals, clinics etc. to install and make use of within their organization. The records created are owned by the care giving organization which can choose to share certain parts of it with the patients (Garets and Davis, 2006).

The NAHIT also defines Electronic Health Record (EHR) as:
"The aggregate electronic record of health-related information on an individual that is created and gathered cumulatively across more than one health care organization and is managed and consulted by licensed clinicians and staff involved in the individual's health and care." (Neal, 2008)

An EHR on the other hand is a systematic collection of a subset of various EMR's of a particular patient from the different care giving organizations that the patient has visited. It is owned by the patient, allowing patient input and is created as a patient's health history record (Garets and Davis, 2006). This however is a process that evolves over time as the record is only built up with data from previous EMR records from the different care giving organizations.

B. HIPAA & HITECH Background

It is evident that the healthcare industry in particular is susceptible to data fraud and medical identity theft owing to the nature and content of the data it creates, collects, and stores. Personal and sensitive data such as SSNs, insurance details, payment information, and medical provider information along with the past medical history enables criminals to file fraudulent claims that often go undetected for long periods of time, and when finally identified have already caused great problems for people concerned.

Passed by the US Congress as early as 1996, the Health Insurance Portability and Accountability Act (HIPAA) is a set of uniform standards established to protect the privacy and security of health information of patients, to combat abuse and fraud in health insurance, and to grant people rightful access to their health information. It was initially passed to be followed by doctors, hospitals, and other healthcare providers, and has moved on to extend the liability of the privacy and security compliance furthermore to covered entities and business associates.

According to healthit.gov website (November 2013), the Health Information Technology for Economic and Clinical Health (HITECH) act was enacted to encourage the adoption and use of EHR's and IT in the healthcare industry. After this act was passed, the healthcare industry has

been compelled to adapt to the offerings of the IT world. Also, the American Recovery and Reinvestment Act of 2009 (ARRA) provided incentive payments to eligible medical professionals and hospitals participating in Medicare and Medicaid programs. They were encouraged to adopt and successfully demonstrate the meaningful use of certified EHR technology to achieve their goals by making use of the technological advancements in the healthcare IT industry.

SENSITIVE PATIENT INFORMATION AND INFORMATION TECHNOLOGIES

We have already understood the inherent nature of sensitive data in the healthcare industry and now-a-days every encounter with the healthcare system results in an electronic footprint. In the United States, where the healthcare industry is data-rich, a large amount of data is stored electronically and there is a need for a well-defined system and coordination process to handle this data. Further, aiming towards seamless connectivity of electronic and personal health records, home monitoring, distance medicine, etc. only means multifold increase in data with which comes increased prospects for violating privacy and security of personal health information. We shall take a brief look at the different mediums in which electronic data is stored and made available, use of mobile apps, cloud computing and big data technologies to capture, store, disseminate and analyze health information and finally IT practices that are used to manage this data.

Healthcare data on personal computers and removable storage devices

Medical personnel are increasingly delivering mobile care both inside and outside care giving organizations and the use of a wide range of portable devices like personal computers or laptops, most often with removable storage devices like a CD/DVD or USB keys to store and maintain patient data has become almost ubiquitous.

Many companies are developing software and IT infrastructure platforms for healthcare providers to seamlessly achieve their goals. The amount of patient information and patient encounter data created, stored, maintained and shared using these systems are abundant and hence it is crucial to have adequate security measures like built in password security and authentication checks along with a reliable IT infrastructure to integrate these systems together.

In highly complex environments like the health IT systems where one cannot restrict the number of devices being used for storing and transferring sensitive patient data, there must be multiple layers of security to prevent malicious attacks from various sources. The first and most important task must be to secure devices with strong password protection to avoid misuse of data in case of loss or theft of the device itself. Predetermined security software installation in the devices used must be made mandatory before connecting to the hospital's network in order to prevent virus and malware attacks. Access control also must be enforced to restrict the data access to each individual based on their designated tasks. This prevents misuse of data by people within the organization.

It is commonly accepted now that data stored in removable devices such as a CD/DVD or USB keys must be encrypted while saving to the device, again to prevent misuse of data in case the device is lost. Data leaks must be monitored and controlled by performing regular data usage pattern checks on the devices registered with the network. Most importantly, a centralized data

management methodology should be maintained to ensure data protection from different sources as the data stored in the network is made accessible to various stakeholders.

Healthcare data using Mobile Apps

The growing use of mobile devices in daily life activities is not uncommon and the healthcare industry is not exempt from this development. This only makes compliance with laws like HIPAA & HITECH acts more challenging and important than ever. The fact that electronic communications are swift and asynchronous exchange offers many advantages to physicians and care givers in this fast-paced world, to effortlessly exchange clinical information via pager messages, short message service (SMS) through mobile phones, or messages and emails sent via smart phones.

Though convenient, texting patient health and patient care information from devices with inadequate safety features can expose an organization to potential privacy and security threats, paving way for unnecessary legal and financial consequences for the organization. As mobile devices and their applications generally lack encryption, data sent using such devices are not secure. In most cases, the sender cannot verify if the message has been sent to the appropriate receiver or even sent successfully. Telecommunication vendors or wireless carriers may choose to store the information sent using their services and thus have access to data sent. The loss or theft of a mobile device containing unsecured protected health information has been a source of numerous reported breaches in the recent past (Hardiman and Edwards, 2013).

Therefore, it is typically not advisable to use mobile apps and services to send messages pertaining to critical patient health information, to ensure lawful protection and promote better security of healthcare data unless adequate precautions are taken to secure the data sent through specific applications.

Healthcare data on the Cloud

Healthcare IT News (2012) defines cloud computing as a means of delivering hosted services over the Internet to store, manage and process data, rather than on a local server or personal computer. While the concept of cloud based servers and virtual machine software as a service has been a popular across industries for many years for promoting ease of data storage solutions, small or large, at very competitive prices, security and data breaches are still a concern for one and all.

For the healthcare industry, the concerns with adapting to cloud based computing and virtualization software are many. The main issue is with the ever-changing government mandates as a result of which the IT teams find it difficult to support unforeseen changes. The white paper VMware vCloud® for Healthcare and HIPAA/HITECH (2013), notes that another compelling factor is the company's difficulty in managing large information flow between their multiple applications to create and monitor patient data. Also, the fact that caregivers have started using various devices on-the-go to provide ongoing care to their patients has made device portability and secure access to data mainly from authorized devices highly critical. To overcome these obstacles, healthcare providers are embracing the use of cloud based devices to store and manage their data in an effective manner.

Companies like VMWare (2013, 2012) have developed the virtual desktop infrastructure, where the patient data is stored in a cloud based datacenter, instead of on the originating device

itself. Hospitals then will not have to worry about sensitive patient information being lost when the device itself is being misplaced.

Using the cloud based technology also makes the healthcare system easily scalable as virtual memory can be increased and decreased on-the-go with ease without causing any disruption to the existing users.

Data centers are extremely expensive to maintain by hospitals as they need to have their own IT department and equipment to support their vast IT requirements. Having virtualized cloud based systems reduces costs and promotes ease of use and maintainability of IT systems for hospitals.

In spite of all this, there is the obvious concern of storing data somewhere outside the control of the hospital where they cannot ensure its reliability. Also, bearing in mind the fact that cloud computing is mostly dependent on a working internet connection, the only other concern in adopting this is the fact that the hospitals or designated care givers must have an uninterrupted access to a fast paced internet connection.

Big Data Analytics

Reliance on medicine and progress in the field of medical sciences has saved numerous lives over the years. This knowledge has progressively been documented and passed on through generations. With advancement in technology, storage and distribution of this knowledge has become easier. The same technology has made storing and deciphering from healthcare data of patients more optimum and personalized. With progressive adoption of electronic healthcare records and the use of computers and tablet devices by healthcare providers on a daily basis, medical data analysis using Big data analytics offers breakthrough possibilities for new research and discoveries, better patient care, and greater efficiency in the health and health care industries.

In simple terms, big data "is data that exceeds the processing capacity of conventional computational resources due to its size and speed which do not fit the structures of regular systems architecture" (Dumbill, 2012). Big data's defining features include the ability to handle massive data volume and variety, at high a velocity. Processing of Big Data to retrieve meaningful information at extremely quick speeds is called big-data analytics. This is made possible with the presence of new, flexible, and easily expandable infrastructure in the IT field, including so-called data lakes and cloud data storage and management solutions (Roski, Bo-Linn, and Andrew, 2014).

To better explain the use of Big Data in today's world in the healthcare industry, let us consider the example of a health app on a smart phone device. On installation of the app, the owner of the device enters basic body statistics like age, sex, height, weight, blood pressure, blood type, blood group, dietary habits, and so on. The app on the other hand collects this array of information on a continual basis, keeping track of various parameters and its variations based on the user's input. It then analyzes these trends, makes calculations on the varying parameters and finally provides suggestions for a healthier lifestyle. The ease with which this huge cache of data is successfully managed and efficiently processed is achieved by the use of Big Data analytics. The use of Big Data also necessitates making this data available across the users' multiple devices and providing access to this data over the web. For the health conscious people in today's technologically advanced world, Big Data analytics collates relevant data across millions of users and makes predictions on the lifestyle and activity requirements on a daily basis.

When such is the power of big data on a small smart phone device, one can imagine how this can be used for predictive analysis in various other lifesaving fields such as drug analysis to cure diseases and disease control, to shift towards an evidence-based pre-emptive treatment rather than reaction based. This could greatly help curb the number of people impacted by health issues. Healthcare providers and drug makers are equally benefitted by sharing and compiling such information in order to help the industry as a whole to move in the right direct with their research and analysis.

However, with such great advantages, major downsides come hand in hand. For Big Data to be successful, the healthcare industry must make changes at its core to maintain and protect the privacy of the sensitive patient/user information. With hackers vying for access to all kinds of data, it is extremely important to provide adequate security measures for retrieving, adding and modifying user data. If the healthcare industry wants to fully utilize the features offered by Big Data analytics, it is essential that standards are established on how data should be collected, processed, and finally discarded when it is no longer needed. In addition, the use of unstructured data and fast quick data retrieval using technologies such as NoSQL are insecure by design in the current Big Data ecosystem. The potential of Big Data is aplenty and so are the challenges.

Outsourcing healthcare IT work

Corporations have always had a tough time trying to decipher ways to reduce cost and in turn increase profits for themselves and their shareholders. They struggle to decide on what services they can provide most economically internally and which services are more cheaply obtained from some source outside the company. Organizations have extensively been sourcing their non-critical processes through external service providers to achieve division of labor and focus on specialization. This process popularly known as Information technology/business process outsourcing is done to reduce costs and get the work done from independent vendors or subsidiaries of their own company from an external country where labor costs are lower (Punke, 2013).

Depending on the complexity of the organization's functions, they decide what part of their work is to be outsourced and which part to handle internally. While many industries have started experimenting with outsourcing for a long time now, the healthcare industry took rather cautious steps towards this venture, again in the best interest of the security of sensitive patient information (Lacity et. al, 2011).

While healthcare companies are increasing their budgets for IT expenses, they are still restricted by various other factors that need their attention, like recruiting qualified staff, upgrading their facilities, growing regulatory requirements, pressure to provide the latest medical technology, and increasing costs for insurance malpractices (Jacobson, 2004).

Ceasing this opportunity, outsourcing companies market for healthcare providers to outsource smaller aspects of their work such as network & IT support, website/applications development, medical transcription, and call center facilities for lesser critical processes to other countries to cut down operating costs.

However, like any other form of healthcare IT, outsourcing also creates the potential for identity leaks and associated threats. As not all countries have healthcare rules like the HIPAA and HITECH laws enforced like in the United States, ensuring compliance with the outsourcing company and its employees may be a very challenging task.

Another major issue with the success of this model for healthcare systems is the criticality of turnaround time for the processes outsourced. For example in the case of medical transcription, the patient's health history must be up-to-date at any given point in time and cannot experience a time delay due to outsourcing activities or time differences between countries in different geographical locations. Managing this might be a cause of concern for hospital authorities as these changes reflect directly on the hospital's patient care applications for providing appropriate and continuous patient care.

To address all of the issues listed above in section III, the Final HIPAA Omnibus rule effective from March 2013 extended direct liability for HIPAA violations to include business associates. This strengthened the penalties for HIPAA violations and made covered entities and business service providers also liable, thus ensuring protection of patients' privacy, regardless of where their information is stored, and who it is accessed and maintained by (Canellos, 2013).

ENSURING HEALTH IT SECURITY

The earlier sections discussed technology and practice options available for Healthcare IT delivery and the legal issues posed by these choices. Based on the earlier discussion and the available best practices used in the industry we recommend some of the mechanisms one can adopt for ensuring safety in creating and maintaining electronic patient records next.

- The first consideration in implementing healthcare IT practices for a hospital or care giving organization is to perform a realistic valuation of the patient data they hold or propose to collect in the future, and determine their use for IT systems. This is essential to evaluate their requirements and to formulate a well-defined IT plan which is on par with the organization's needs and government regulations.
- Once the plan is created, the organization needs to identify a suitable vendor to convert their plan into reality. The IT vendor should have the competency to implement and test all of the hospital's requirements with due diligence, at competitive costs and in a suitable time period.
- Identifying and finalizing the system architecture is very important to successfully create an IT infrastructure to support the large systems for the hospital with appropriate network connectivity and client-server architecture required for the data exchange.
- The different systems that are involved in the patient's treatment process should be integrated seamlessly to allow efficient data flow while maintaining data integrity.
- Data maintained in the hospital's repository must be in a format that is portable across platforms and compatible with future software and hardware updates.
- Each device connected to the hospital's network must have sufficient encryption techniques to handle any unforeseen data breaches.
- The devices should also be configured to perform regular data backups with the data repository to maintain uniformity of information across devices.
- Outsourcing certain processes is one of the cost cutting measures for the management and should be carried out by cautiously weighing all its impacts.

While these are some of the considerations for implementing a successful healthcare IT system, the challenges are aplenty and so are the opportunities for improvement. Each organization should gauge their stand and rightfully determine their individual requirement without making any compromise on quality of their systems to maintain the security of their data.

CONCLUSION

The influence of Information Technology has changed the working model of all the major industries in the recent years. Majority of the population today has learned to adapt to these evolving traditions and is ready to accept more radical alterations in the near future. Among the major industries, IT for healthcare is both complex and critical and has been a challenge to the government responsible for making the regulations, the hospitals and physicians who are getting accustomed to its new ways, and more importantly to the companies and individuals who are involved in merging IT with healthcare. With health IT producing applications that are aiding the doctors like never before, better treatment to patients has become a norm. A number of cutting edge healthcare applications for Preventive care, Diagnosis and Follow-up treatment certainly have facilitated to save more lives but at the same time challenges to carefully save the patient's sensitive data, sharing patient's data across different platforms, adopting an approach to satisfy all the guidelines prescribed by the government, and avoiding cases of technical error leading to human error are some of the common factors which have kept this transition from being a complete success.

According to a blog from Global Scape Inc. (2013), the initial unsuccessful implementation and deployment of the healthcare.gov website responsible for insurance exchange of the Affordable Care Act is a classic example that depicts the problems of implementing a healthcare IT system with complex compliance issues. It has been contended that the security measures taken to build the system was inadequate, resulting in problems like user information being sent to untargeted recipients, and the web-site itself being vulnerable to attacks. A company like Google which has been a forerunner in the field of internet technologies with its innovation and having changed the face of Internet since its inception, decided to pull the plug on its short lived personalized health information centralized service Google Health since it did not have the expected impact. While it is a concern that a company with such high technical expertise and infrastructure found it difficult to adapt to and satisfy all the requirements of the healthcare industry, it is reassuring that the same company has made a comeback with its most innovative product the Google Glass, which can be used for benefitting health IT in numerous ways (Perna, 2013).

While adapting to newer technologies is essential, violations of government regulations may not only cause the disclosure of patients' sensitive information, but can also bring about tremendous monetary loss and damage to the healthcare providers' reputation. Thus, taking effective measures to address this gap should be the most critical requirement for all healthcare entities; bearing in mind the complexity of such regulations.

REFERENCES

(November 2013). *U.S. Department of Health & Human Services.* Retrieved November 20, 2013 from http://www.hhs.gov

(November 2013). *HITECH Act Enforcement Interim Final Rule.* Retrieved November 20, 2013 from the http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

(November 2013). *HealthIT.gov.* Retrieved November 21, 2013 from http://www.healthit.gov/

H Neal. (2008, November 14) *EHR vs. EMR – What's the Difference?* [Web log comment]. Retrieved November 20, 2013 from http://profitable-practice.softwareadvice.com/ehr-vs-emr-whats-the-difference/

D Garets and M Davis. (2006, January 26). *Electronic Medical Records vs. Electronic Health Records: Yes, There Is a Difference*. A HIMSS AnalyticsTM [White Paper]. Retrieved November 20, 2013 from http://www.himssanalytics.org/docs/WP_EMR_EHR.pdf

(November 2013). *Meaningful Use Resources.* Retrieved from http://www.healthit.gov/policy-researchers-implementers/meaningful-use-resources

(2013). Endpoint Data Protection - A Top Concern for Healthcare Providers: The Stimulus Act Creates New Priorities for Quality of Care, Patient Safety, and Compliance. *Guardian Edge* [White Paper]. Retrieved November 15, 2013 from http://www.ihealthtran.com/pdf/Guardian%20Edge.pdf

M Hardiman and T Edwards (2013). *Clarifying the Confusion about HIPAA-Compliant Texting.* [White Paper]. Retrieved November 15, from http://www.perfectserve.com/connect/sites/default/files/white-paper-pdfs/clarifying_the_confusion_about_hipaa-compliant_texting.pdf

(2012). Healthcare IT News. Retrieved November 17, 2013 from http://www.healthcareitnews.com/directory/cloud-computing

(2013). *VMware vCloud® for Healthcare and HIPAA/HITECH.* [White Paper]. Retrieved November 18, 2013 from http://www.vmware.com/files/pdf/solutions/VMware-vCloud-for-Healthcare-HIPAA-HITECH-White-Paper.pdf

(2012). *VMware Point of Care Solutions for Clinicians and Caregivers.* [White Paper]. Retrieved November 18, 2013 from http://www.vmware.com/files/pdf/Vmware-Point-of-Care-Whitepaper-en-wp.pdf

E Dumbill, (2012, January 11). *What is big data?* [Online] Retrieved November 18, 2013 from http://radar.oreilly.com/2012/01/what-is-big-data.html.

J Roski, G W Bo-Linn, and T A Andrew (2014, July). Creating Value in Health Care through Big Data: Opportunities and Policy Implications. Health Affairs, July 2014, 33 (7), 1115-1122. doi:10.1377/hlthaff.2014.0147

H Punke, (2013, October 04). Outsourcing is Exploding in Healthcare — Will the Trend Last [Online]. Retrieved on November 25, 2013 from http://www.beckershospitalreview.com/workforce-labor-management/outsourcing-is-exploding-in-healthcare-will-the-trend-last.html

M C Lacity, S Solomon, A Yan, and L P Willcocks (2011). Business process outsourcing studies: a critical review and research directions, Journal of Information Technology, 26, 221–258. doi:10.1057/jit.2011.25

T Jacobson (2004, June). IT Outsourcing in US Hospitals: Potential Benefits and Risks, *Research Gate.* doi:10.1.1.200.5433

D Canellos (2013, October 10). How HIPAA affects healthcare cloud computing decisions [Online]. Retrieved on November 23, 2013 from http://healthitsecurity.com/2013/10/10/how-hipaa-affects-healthcare-cloud-computing-decisions/

(2013, November 1). Healthcare.gov shortcomings generating significant data security concerns, [Web log comment] *Global Scape*. Retrieved December 01, 2013 from

http://www.globalscape.com/blog/2013/11/1/healthcaregov-shortcomings-generating-significant-data-security-concerns

G Perna (2013, November 13). 20/20 Vision: Google Glass in Healthcare is Coming, [Web log comment] *Healthcare Informatics.* Retrieved on December 02, 2013 from http://www.healthcare-informatics.com/blogs/gabriel-perna/2020-vision-google-glass-healthcare-coming