Journal of International Technology and Information Management

Volume 23
Issue 3 *Double Issue 3/4*

Article 10

2014

Electronic Health Records: Challenges and Opportunities

Jaymeen R. Shah
Texas State University

Mirza B. Murtaza
Georgia Gwinnett College

Emmanuel Opara
Prairie View A&M University

Electronic Health Records: Challenges and Opportunities

Jaymeen R. Shah
Department of Computer Information Systems & Quantitative Methods
Texas State University
USA

Mirza B. Murtaza
School of Science and Technology
Georgia Gwinnett College
USA

Emmanuel Opara
Department of Accounting, Finance & Management Information Systems
Prairie View A&M University
USA

ABSTRACT

During the last three decades, healthcare expenditure in the U.S. has substantially increased. If this pace of increase is not controlled, it will lead to disastrous results for the healthcare system. An effective use of health information technology would not only improve the quality of healthcare but help reduce healthcare costs considerably. However, risks of privacy and security of patient electronic health records are great. It is recommended that healthcare organizations use IT management best practices, follow proper risk assessment and management guidelines, and keep up with latest technological advances to ensure the privacy and security of patient data.

INTRODUCTION

Medicare reimburses physicians for the services provided using a fee schedule referred to as the 'Resource-based Relative-value scale'. This scale was created with the intent of calculating relative prices for the services rendered by the physicians based on the amount of work associated with providing each service, the average practice expense involved, and geographic location adjustment factors. To control cost of physician reimbursement, the resource-based relative-value scale is combined with a spending limit referred to as sustainable growth rate (SGR). During 2014, physicians are likely to experience an approximately 24% reduction in physician fees as a result of the SGR formula used to compute Medicare's physician reimbursement (Centers for Medicare & Medicaid Services, 2014). To avoid continued use of the SGR formula that could result in reimbursement reduction for services provided by the physicians, recent bipartisan efforts have been focused on the development of an alternative reimbursement system that rewards physicians who improve the quality and effectiveness of care provided to patients (Wilensky, 2014). These bipartisan reform efforts aim to simultaneously attain the goals of improving healthcare quality and efficiency, and controlling healthcare costs.

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

The exponential growth in the U.S. healthcare costs, if not controlled, will impair future economic growth and stability. Over the past three decades, healthcare expenditure in the U.S. has substantially increased. In 2008, U.S. healthcare expenditure was over $2.3 trillion, approximately 16.2 percent of the Gross Domestic Product (GDP). This amount is over three times the $714 billion spent in 1990 and over nine times the $253 billion spent in 1980 (Kimbuende et al., 2010). Government forecast suggests that in 2019 U.S. healthcare expenditure will be about $4.5 trillion, approximately twenty percent of the GDP (National Health Expenditure Projections 2009-2019). Such increase in healthcare expenditure is unsustainable, and if not controlled it will lead nation's healthcare system close to bankruptcy. Sadly, in spite of spending the most on a per capita basis, U.S. ranks well below other developed nations in important healthcare measures such as infant mortality (DeNoon, 2008). A recent report comparing the healthcare performance of seven developed countries (U.S.A., Britain, Canada, Germany, Netherlands, Australia and New Zealand) ranked the U.S. last. Findings of this report confirm that much of the money may not be well spent, as the U.S. ranked poorly with respect to healthcare quality, efficiency and safety (Fox, 2010).

Although the adoption of electronic health records in hospitals and medical offices is not yet universal, but seemingly pace of adoption has been accelerating (Porter, 2013). Widespread adoption and improved use of information technology has been promoted because of its potential to effectively manage health information and efficiently share it between service providers. Proponents of health information technology assert that effective health information management is an important mainstream issue that has the potential to improve the quality of healthcare, reduce healthcare cost, and provide doctors and patients with real-time access to patients' health information. To achieve these goals electronic health records (EHRs) will play an important role. Although EHRs is one of the crucial elements for improving healthcare quality and curbing healthcare cost, the current state of health information records management at many clinics and doctors' offices is comparable to the state of locomotive engines – antiquated. It is estimated that medical records of 90% of the patients are recorded on paper, and most of the prescriptions are written on paper (Carey & Holahan, 2008). One of the main reasons for this is the cost of implementing and maintaining EHR management and e-prescription systems. Approximately seventy-five percent of the physicians in the U.S. practice in offices with ten or fewer doctors. Many doctors' offices in this category have not implemented EHR management systems mainly because of the high initial cost of implementing an EHR system, which can be approximately $30,000 per physician (Lohr, 2009). This amount includes the cost of software, computers, printers, network setup and installation, but does not include the time and effort doctor's office staff devotes to implement and learn an EHR system. In addition to the initial implementation cost, there is an ongoing annual maintenance cost.

To overcome the cost hindrance, the American Recovery and Reinvestment Act (ARR Act) of 2009 provides financial incentives for doctors, hospitals and regional-health-information networks to implement and use EHRs management systems. One of the main purposes of this incentive payment to a physician who demonstrates meaningful use of EHRs is to repay the initial cost incurred to implement an EHR system. This incentive can be approximately $44,000 per physician, which seems adequate to cover the initial system implementation cost. The Congressional Budget Office has estimated that the total of incentive payments to service

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

providers such as doctors and hospitals would be approximately $34 billion. It is hoped that the incentive payments together with the federal requirement to use EHRs will persuade the service providers to transform all health information into electronic records. As the goal is to complete the transition to EHRs by 2014, starting from 2015 doctors and hospitals not using EHRs will incur financial penalties (Pear, 2010).

There is a growing expectation that the overall impact of the ARR Act of 2009 will result in radical changes in the health information management and a major overhaul of the government and service providers' health-information-management systems. This transformation in health information management is likely to result in significant fiscal and societal benefits due to the reduction in healthcare delivery cost and improvement in the quality of healthcare delivered. Billions of dollars allocated for developing EHRs and Nationwide Health Information Network (NHIN) is expected to achieve the ability to share patients' health information between service providers, government agencies and other organizations that need it. To fulfill this vision of electronic exchange of health information between various healthcare organizations, it is essential that a standards based health-information technology be adopted across the nation. This will require creation of standards related to electronic health information to standardize the definition of common medical tasks, procedures, processes and patient data records and a common framework for the NHIN (Havenstein, 2005). Adoption of these standards across the healthcare industry is critical to attain interoperability between the disparate health-information-management systems used by various service providers without the need for developing and maintaining brittle and expensive interfaces between these systems. The eventual ability of the health care service providers' health-information-management systems to exchange and integrate patients' information will improve the efficiency and quality of patient care delivered, and result in an annual savings of more than $77.8 billion in the U.S. (Babcock, 2005). However, it is not clear to the management how they can ensure that all the benefits of EHRs are achieved while providing the required privacy and security to the patient records. The top five healthcare IT issues identified by CIOs in healthcare include the following: 1) Implementation of electronic medical records, 2) Change management from paper to electronic medical records, 3) Reducing healthcare errors with information technology, 4) Privacy of electronic records and 5) Security of electronic records (Palvia et al., 2012).

This paper provides an overview of EHRs and the legal, privacy and security issues associated with the adoption of EHRs. The remaining paper is structured as follows. First, the authors provide a brief literature review that includes the factors driving the use of EHRs, followed by discussion about issues related to the storage of patients' health information in digital form. Next, the legal issues associated with the use of EHRs are presented, which is followed by discussion of the privacy and security issues and requirements of EHRs. Finally, concluding remarks summarize the needs and expectations for successful implementation and use of EHR systems.

LITERATURE REVIEW

To control healthcare costs, the sustainable growth rate formula (SGR) has been used since 1992. The Medicare reimbursement to the physicians is based on the fee-for-service system. One of the main concerns with reducing the amount of reimbursement for the services provided by the physicians is the increase in the number of services provided to the patients in order to recoup the difference in their income due to the reduction in reimbursement provided by Medicare (Wilensky, 2014). As the baby boomers retire and approach the age after which they may require more medical services, government agencies are bracing for more healthcare spending. Thus, there is a renewed concern and urgency for finding alternative ways to reduce the healthcare spending by making it more effective and efficient. The use of EHRs is one of the important elements within the overall solution for reducing the healthcare costs. Storing patients' data in digital form can enable integration and sharing of data between medical facilities at which patients are treated. This can lead to reduction in unnecessary repetition of tests performed, increase in the amount of patient history available to the physician, and enhance the overall quality of care physicians can provide due to the amount of data available for the patient being treated. However, the use of EHRs require that patients' information is stored in digital format and shared with other medical facilities digitally. This requires considerations regarding storage of patient information, and its privacy and security. The following sub-sections discuss issues related to the use of EHRs.

Patients Data Storage

Hospitals and the medical institutions are now implementing the electronic medical record (EMR) technology. An electronic medical record is a digital form of a paper chart that contains a patient's medical records from one practice and serves as a data source for the electronic health record. This technology is very beneficial to the medical practitioners because it can store patients' data in digital form. Having access to patients data in digital format enables the medical practice to track patients' data over time, identify patients who are scheduled to be up for preventive visits and screenings, monitor how well patients measure up to specific parameters of interest to the physicians, and enhance the overall quality of patient care provided by the practice. Data stored in the electronic medical records (EMRs) can be combined to provide the medical practitioner a comprehensive patient history that extends beyond the data collected in the provider's practice area.

It is expected that by 2015, all individuals in the U.S. will have their health information stored electronically. The American Health Information Community (AHIC) has recommended the storage and integration of patients' genetic data within their EHRs and/or PHRs (Personal Health Records) to enable doctors to match available medical treatments with patients' genetic characteristics to select the most effective treatments (Health Management Technology, August 2008, pg. 9). Pharmacies have advocated the use of e-prescription systems, which will permit them to receive, dispense and archive electronic prescriptions. This will reduce paperwork, improve efficiency and accuracy of prescription processing, warn of possible drug interactions, and provide access to prescription information to authorized individuals. However, the use of electronic records that can be easily accessed and processed by the healthcare service providers and other organizations raise concerns regarding the erosion of privacy and security of patients'

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

health information. Shift towards the use of electronic health information require scrutiny of the privacy and security protections for patients' EHRs, PHRs, genetic information and other health related information. Lawmakers are aware of the privacy and security risks associated with the use of EHRs. Several steps have been taken to address patients' privacy and security concerns. Federal privacy and security laws now apply to medical service providers and their business partners, and vendors of electronic health information systems. Service providers and users of patients' EHRs are required to notify individuals affected by a security breach of health information and forbidden from selling patients' EHRs without their consent. In addition, based on AHIC's recommendations, stringent policies and processes are required to safeguard EHRs. Stiff penalties have been introduced for any violations of privacy and security policies (Modern Healthcare, 2009). These new requirements are in addition to the Health Insurance Portability and Accountability Act (HIPAA) requirements for maintaining privacy and security of patients' information. In spite of these actions, there are major concerns regarding the inadequacies of the current policy development and legal remedies available to deal with the many important privacy issues created by the move from a fragmented and mostly paper-based health-record system to an integrated EHRs system (Rothstein, 2007).

Health Records in the age of the Internet

According to the Code of Ethics adopted by American Medical Association, "The physician should not reveal confidential information without the express consent of the patient, subject to certain exceptions which are ethically justified because of overriding considerations." (AMA, n.d., Opinion 5.05). The exceptions obviously involve a patient revealing intent to harm others, etc. The technology use has increased in all areas including the medical profession, so physicians and other health care professionals can store and access the information of patients on their networks and systems. The major challenge among the health care providers now is how to utilize the technology while ensuring the privacy and confidentiality of data.

The privacy issues are significant in the healthcare area, as patients would not want the details of their condition to be available to undesired individuals. With the growth of electronic health records (EHR), it is possible to share patient information with various parties involved in the health care process. EHR implementation has been suggested as a means to improve the quality of care and productivity of healthcare professionals (Evans et al., 2006). The impacts of using EHR include cost, paperwork and healthcare error reduction, remote and easy access to patient data, improved patient-provider relationships, and mitigation of credibility and privacy concerns (Mukherjee & McGinnis, 2007). Through the use of virtual networking, physicians and other healthcare providers can access patient information from any place and at any time. EHRs include patient charts, reports and other records that are essential for quality of care at the point of care.

There are many external requirements that impact the way organizations deal with health records including the mandates from the HIPAA, state regulations and the industry best practices. According to Appari and Johnson (2010), there are about sixty state-level laws enacted that involve healthcare records. Healthcare is a huge sector in the US. It is not just the primary organizations like hospitals, physicians, laboratories and clinics that are involved. But there are other industries that have stakes in health-care delivery like pharmaceutical companies, insurance

companies and medical research institutions. Easy access to patient data including their conditions, treatments and procedures will be beneficial to all of these organizations as well as to the public health organizations that work to prevent situations that are potentially epidemic and catastrophic, for example in preventing the spread of flu. Public officials can analyze and track trends of the care and medications prescribed. Additionally, availability of complete medical histories to the primary and emergency care providers may produce better care for the patients.

The privacy threats are classified into two major categories, namely, organizational threats and systemic threats (Appari & Johnson, 2010). Organizational threats could involve inappropriate or malicious access by internal or external actors. This involves employees within the organization or someone external who can illegally access the internal systems. On the other hand, systemic threats refer to use of data by an authorized agent but for a purpose beyond the original intent. Some organizations might have access to medical information about patients including procedures and treatments performed, that would allow them to direct resources to certain healthcare areas or target patients who require the medications and treatments. But this may compromise patient privacy, and may or may not be legal.

Patients' health information is valuable and the value would continue to grow since the health care industry is big business. It seems that it is possible that medical information could be sold, as the customer addresses and shopping records are sold. Thus, it is a major challenge to maintain privacy, security, integrity and availability of patient information in the face of pressure for information sharing. To tackle these challenges, organizations must establish enforceable policies, rules, guidelines, and procedures and also implement technological solutions that focus on and protect from latest data security issues.

LEGAL ISSUES – FEDERAL (HIPAA) AND STATE

During 1990s, the US government identified health information technology and systems as critical to any revolutionary changes in healthcare. The potential benefits from these technologies included the reduction of paper work and in all important medical errors area. Having access to a patient's medical history and the healthcare provider's ability to view health information would improve patient diagnostics, public health outcomes and minimize the chance of adverse drug interactions.

There are concerns regarding the protection of the vast amount of data and information transmitted from a wide range of sources, ensuring the integrity of the data and making it available to various healthcare professionals, staff workers, and patients is not a small task. Healthcare organizations, like financial institutions, do have some strong reasons to protect private medical information; however, it requires presence of controls and oversight of the procedural, technical and physical systems. Federal and state level regulations along with industry standards must provide the guidelines for how to handle, access, and use data along with how to enforce the security measures.

According to Clarke et al. (2009), the potential issues that patients may face include: a) Privacy and Integrity of Health Related Data, b) Security Breaches, and c) Medical Identity Theft. The HIPAA Privacy Rule provides federal protection for personal health information held by entities

and provides patients' rights with respect to their information. A key to this rule is that it permits the disclosure of personal health information when needed by an authorized person. The HIPAA Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information.

The privacy and security of medical information is getting a lot of attention because of its personal nature, its significance, and the potential impact if the data is used in a malicious way. Anyone who handles or has access to medical information will require specific training for his/her responsibilities. HIPAA addresses the protection of patient records in all forms. However, HIPAA itself does not have major provisions to protect medical information since there are weaknesses in the enforcement guidelines. ISO 27799-2008 standard provides guidelines that are more stringent and includes the guidelines on the use of internet and wireless technologies to share personal medical information, and focuses on confidentiality protection. Also, this standard focuses on making information more secure. So the purpose of ISO 27799-2008 standard is to assist health organizations in adopting a better IT security stance (ISO 27001, 2011). HIPAA was designed to protect privacy; however, it does not provide any guidelines on the mechanisms of protection, which would be beyond the purview of any law. That has to be developed as a standard by the industry itself.

The HIPAA legislation is primarily concerned with the Electronically Protected Health Information (EPHI). The US Dept. of Health and Human Services has developed a framework to apply HIPAA to EHRs, with implementation of the regulations to all covered entities that use EHRs. The objective of health information security is to assure the confidentiality, integrity and availability of a covered entity's information systems. This does not distinguish health information security objectives from those of other areas of operations outside of healthcare. But when it comes to health information security, there is a low threshold before a given operation becomes critical to the functioning of the entity as patients' lives and wellbeing as well as their privacy are entrusted to the reliable functioning of health-care information systems. Although HIPAA is concerned with the privacy and confidentiality of health records, the other components of integrity and availability are also strongly related and hence in the purview of this legislation. The Dept. of Health and Human Services (HHS) interprets HIPAA as a multi-faceted approach to health information security in relation to EHRs.

According to Kam (2012), HIPAA and HITECH (Health Information Technology for Economic and Clinical Health Act) are intended to safeguard protected health information. Table 1 summarizes some of the changes made by HITECH Act in order to strengthen privacy and security of protected health information (PHI). Additionally, most states have privacy and security breach notification laws. President Obama offered Consumer Privacy Bill of Rights in 2012, which provides people with an understanding of what to expect from companies that handle their personal information, as well as a set of principles for companies that use personal data. However, HIPAA-protected PHI does not benefit from the Consumer Privacy Bill of Rights and is subject to some privacy pitfalls (Kam, 2012). Maintaining trust is essential to any successful business, especially it is critical for healthcare system due to its significance. According to HHS, about half a million patients did not seek earlier cancer treatment and about two million people did not seek treatment for mental illness because of the privacy concerns.

The major areas of the privacy and security approach under HIPAA include administrative controls, physical controls and technological controls. It is important to note that some of these controls are required while others are considered as best practices, so they are addressable but not mandatory in any strict sense. Administrative controls are dependent on the organization itself and relate to its culture and how the entity perceives the importance of health information security. Under HIPAA, it is required that the information security policies must be in writing, and a designated privacy officer who is in charge with oversight of HIPAA compliance is also required. An organization must have mechanisms in place to ensure effective management oversight of information security. Also, regular employee trainings and review of best practices help increase information security awareness within the organization. Additionally, it is also required that third party vendors doing business with the organization should also be scrutinized for their compliance with HIPAA.

Table 1: Major changes by HITECH to HIPAA.

Area	**HITECH Modifications**
Audits	Periodic audits by Dept. of Health and Human Services (HHS) to ensure HIPAA compliance.
Data breach notification	Covered entities must notify within 60 days of the discovery by the entity or business associate.
Data breach investigation	HHS must investigate any potential of willful neglect.
Data breach penalties	HITECH fines are $100 to $50,000 per violation, with yearly maximum of $25,000 to $1.5 million and mandatory penalties for willful neglect.
Use of PHI	HITECH requires health care organizations to limit the use, disclosure, or request of PHI, to the extent practicable, to a limited data set or to the minimum necessary.
PHI Disclosure	Organizations that use electronic health records must account for all disclosures, including those for treatment, payment, and healthcare operations. They must account for disclosures made by their associates.
Dissemination of PHI to patient	Organization must provide, preferably in electronic Format. Organizations must provide the patient, and to entities authorized by the patient, with an electronic copy of their medical record.

Adapted from Tanio, C. P. (n.d.). Key HITECH Changes to HIPAA. Maryland Healthcare Commission. Retrieved from http://mhcc.dhmh.maryland.gov/hit/hipaa/Documents/hipaa_hitech_chart.pdf

When it comes to electronic health information, organizations should limit the access to only those employees who require the particular information to effectively perform their duties. Health organizations employ a large number of employees, and there are numerous personnel changes throughout the year, so they must have policies in place to address changes in

authorization of access rights and privileges along with the termination of employee access to electronic health information. Contingency planning is also very important, thus administrative practices should address the need for appropriate contingency plans. Risk assessment, including its identification and potential mitigation in terms of critical functionality to the entity should also be performed routinely. There should be provisions in place in case there is a power outage while a patient is undergoing a procedure. Additionally, an organization may require that a paper backup copy of some records must be available for quick reference in case information resources become inaccessible temporarily due to some disaster. Disaster recovery, incident response and data backup provisions should be established, with periodic testing and appropriate modifications made as necessary. Logging of user activity on the healthcare systems should be required as well as periodic auditing on both a routine and event-based basis to ensure HIPAA compliance.

Regarding physical controls, organization's security plan must address the needs of physical security of the complete network, from central data storage to the various desktop and mobile devices used by employees throughout the organization. Restricting access to work areas by the authorized personnel only is required, logging visitor access, and securing the visibility of data on the communication devices must be ensured. Some other important considerations include safety of mobile devices from potential theft, secure virtual private networking from remote locations and handling of hardware/software by authorized personnel only. Healthcare facilities do use devices that are supplied by vendors and store in them personal health information. Therefore, organization must place controls for vendor compliance, testing and accurate record of installation and removal of such devices on the facility network.

To ensure patient data, technological safeguards must be in place. Based on HIPAA provisions, on any open network, electronic health information must be encrypted, however, this is not a requirement on a closed network. All users must be appropriately authenticated. The organization could be held responsible in case of breach of security, theft or unauthorized alteration of records. The common approaches used to ensure this include using strong passwords, integrity checks and digital signatures. Appropriate use of prevention tools, like anti-virus, intrusion detection and prevention systems, is required. Risk analysis and management approaches must be used and documented, however, no specific methodologies are prescribed.

SECURITY AND PRIVACY OF EHRs

A patient's EHR is a longitudinal and organized collection of his/her health related information (Gunter & Terry, 2005). As EHRs contain patients' personal and sensitive information, it is essential that organizations thoroughly investigate and resolve privacy and security issues concerning the use of EHRs to avoid inadvertent release and misuse of patients' information. Although, the move to EHRs will benefit patients and enable the healthcare providers to deliver efficient and quality healthcare, it also raises privacy and security risks. For example, the use of EHRs enable doctors to access complete patient information when treating a patient from their desks and even remotely, which is important for telemedicine. However, it also allows a hacker to access patient information from a remote location. Most patients know that it is much easier to illegitimately copy, read and share EHRs compared to paper-based health records that are physically isolated with restricted access. Survey of U.S. adults regarding the use of EHRs revealed that approximately sixty-five percent of those surveyed were concerned about the leak

of sensitive health information, increased sharing of patients' health related information without consent, and easing of existing federal health privacy regulations. Due to the anxiety caused by the increased privacy and security risks of EHRs, it is possible that some patients will not disclose necessary health information to healthcare providers (Merisalo, 2012). To prevent such negative effects of the use of EHRs, it is necessary for organizations to take appropriate steps to alleviate patients' privacy and security concerns by ensuring that patients' information is solely used for the purpose for which it was collected and accessible to only those with their consent. This is critical for positively influencing patients' trust in the use of EHR systems and its long term success.

Patients' trust in EHRs may be affected by various factors such as the healthcare providers' reputation and patients' perception of the risk to the privacy and security of their EHRs. It is possible that patients' perceived risk to the privacy and security of health information is affected by the medium used to record and share health related information. Interestingly, it has been shown that individuals' perception of privacy, security and trust vary between online and offline transactions even when transacting with the same business (Chellappa, n.d.). In the context of healthcare, patients provide service providers (doctors and hospitals) health related information, which is equally or even more sensitive than information shared in online transactions. Trust is a context dependent construct (Gulati, 1995), which is influenced by the characteristics of the medium used to collect and share information (Keen et al., 2000). Thus, it is possible that patients' perceptions of privacy, security and trust will vary between the use of paper-based health records and EHRs, even when a patient visits the same doctor and hospital for treatment.

Although, patients have trusted healthcare service providers with their sensitive personal and health information, patients' concern regarding the privacy and security of this information is likely to increase when it is stored and shared electronically. Concerns regarding risk to the privacy and security of personal information have been cited as one of the main reasons for consumers' reluctance in sharing personal information online and conducting online transactions (Gilbert, 2001; Meeks, 2000). These observations suggest that the use of EHRs and its exchange between service providers may increase patients' perceived risk to the privacy and security of their health information, which could increase patients' unwillingness to provide necessary information to healthcare providers. For successful adoption of EHRs, it is important to prevent manifestation of such possible negative effects of using EHRs and sharing them electronically between service providers. Thus, it seems essential to investigate the effect of the widespread use of EHRs and its exchange between service providers on patients' perceived risk to the privacy and security of their health information. Understanding gained from this investigation can be used to ease the transition from the largely paper-based health records to entirely EHRs-based health information, and to ensure higher-level of acceptance of EHRs by patients without any unwanted negative effects. The following sections explore the effects of the use of EHRs on patients' perceived risk to the privacy and security of their health information and discuss approaches to mitigate these risks.

Privacy of EHRs

Information privacy is defined as an individual's right to decide what, when, how and how much information about him/her is revealed to others (Martin, 1973; Udo, 2001; Westin, 1967). Most

people believe that they should have control of their own personal and health information, and consider its privacy and security important. An individual's information privacy is violated when there is unauthorized collection, disclosure, and/or secondary use of his/her personally identifiable information such as health information (Wang et al., 1998). The expected increase in the use of EHRs might result in more frequent information privacy violations due to inadvertent and intentional dissemination and manipulation of patients' health information. Given the importance of health-information privacy to the long-term success of EHRs, it is essential to understand the effect of the use of EHRs and information privacy violations on individuals' perception of risk to information privacy and their willingness to provide necessary health information to service providers. Researchers have contended that in technology-based environment it is important to study individuals' information privacy concerns and methods that can be used to alleviate these concerns (Miyazaki & Fernandez, 2001; Stewart & Segars, 2002).

To safeguard patients' health-information privacy and control EHR data access and disclosure to third parties (e.g., healthcare providers), patients should be able to articulate privacy and disclosure policies. Enforcement of these policies require implementation of access-control mechanism with auditing capability. As clinical staff, administrative staff, and management staff may require access to patients' EHRs, the use of role-based access control is appropriate as it enables definition of permissions and restrictions based on the role of the staff member (Fernandez-Aleman et al., 2013). Access control rules for staff members must be explicitly defined in accordance with the stated privacy policies and strictly adhered to. These access rules must be updated to determine the EHR data accessible to a user at a specific point in time as detailed access to patient's EHR is provided only to the members of patient's care team. Each staff member must be provided with minimum access necessary to perform his/her tasks (Kahn & Sheshadri, 2008).

In addition to defining the necessary role-based access control rules, it is essential to implement a transaction log to record all EHR access requests and response to these requests by the EHR system. Logging and auditing of access to patient's EHRs will enhance his/her confidence in the enforcement of access-control policies. To prevent tampering of the transaction logs to remove unauthorized access, log files must be stored on tamper-resistant hardware (Haas et al., 2011). The EHR transaction log archive will enable maintenance of access trail, which can be used for access audits. The transaction log data must be periodically analyzed to evaluate EHR data requests and the validity of EHR system's response to each data access request. All inappropriate EHR data access permitted by the system must be investigated to determine its cause. The maintenance of transaction log and analysis of transaction log data enables verification of the access-control policies implemented to preserve patients' health-information privacy.

EHR systems must maintain information about all EHR data disclosures. To protect against unauthorized disclosure of patients' EHRs requires an efficient scheme to trace unauthorized data disclosures to the individual users. Digital watermarking can be effectively used to trace disclosure of EHRs. In digital watermarking, identifiable codes are embedded in the text and images to be traced. Watermarking can be used for fingerprinting users by assigning unique watermarks to each user (Cox et al., 2008). Each EHR data disclosure can be tagged with the user's watermark to relate it to the user who accessed and disclosed the data. Fingerprinting scheme can be used to effectively trace unauthorized disclosure of patients' EHR data (Haas et

al., 2011). Use of these approaches can preserve patients' medical information privacy when EHR systems is used.

Security of EHRs

Use of EHRs by service providers will create large data stores containing patients' information. Frequent news about data breaches and security issues with commonly used software raise patients' concerns regarding the security of their sensitive health and personal information. These concerns are not without merit, as HHS reported that medical data breaches have affected about 8 million patients (Merisalo, 2012). In the interconnected digital world, securing patients' EHRs is a challenging task. Security of EHRs is of paramount importance to ensure patients' and service providers' confidence in the use of EHRs. In healthcare organizations, security breaches can cause significant damage to the organization and to the patient. In worst-case scenario, unauthorized access and willful changes made to patients' medical records by an infiltrator can result in loss of life. Due to the serious consequences associated with the security breach of EHRs, organizations must thoroughly review the procedural and technological aspects related to the security of EHRs.

Medical facilities must ensure that necessary physical, technical and administrative safeguards are implemented to ensure the privacy, security, and integrity of recorded patient information. The physical safeguards put into effect should at least include the isolation of network and storage devices, granting of physical access to the workstations, servers, and network and storage devices only to authorized personnel, and creating backup of patients' data. In addition, it is important to develop procedures for the disposal of machines, disk drives, and network and storage devices.

The technical safeguards necessary include the use of properly configured firewalls and intrusion detection tools, usage of secure transmission modes for remote access and exchange of data (e.g., use of virtual private networks), use of advanced encryption algorithms and methods to store and transmit patients' data, and regular check and installation of software updates. It is best to use both hardware and software based encryption to provide highest-level of security protection to patients' health information (Meingast et al., 2006). To prevent unwanted exposure of EHR data stored and accessed across medical facilities, methods such as private-information retrieval should be used (Chor et al., 1998). Transmission of patients' data between medical facilities necessitates nonrepudiation of data exchange to ensure confidence in the transfer of medical records between the two medical facilities. This requires the ability to record the handshake between the devices, time of the transaction, and record of the patients' data exchanged between the two medical facilities.

Finally, the administrative safeguards focus on the development, implementation, enforcement, and continuous review of security policies and procedures. Appropriate policies and procedures that must be in place include the maintenance and review of system logs, storage, archival, and retention of patients' data, incident reporting and resolution, emergency contingency procedures, and accountability and disciplinary actions for violations of any policies and/or procedures. Furthermore, there should be procedure for authorization, access control, and determination of the appropriate level of user privilege to access specific resources. For example, policy that

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

encompasses prevention of unauthorized access to patients' data may include logging off when leaving the workstation, automatic account logoff after a certain period of account inactivity, periodic change of user passwords, required complexity level of the passwords used, and use of multifactor authentication. In addition, there must be designated individual(s) responsible for creating new user accounts with appropriate privileges and deactivating accounts of users who leave the organization (Kahn & Sheshadri, 2008). It is necessary to properly document policies and procedures for the three types of safeguards, and provide easy access to these policies and procedures to employees. All employees must be provided appropriate training regarding existing policies and procedures and related best practices. This will enhance employees' motivation to ensure that access to EHR system and patients' medical information is granted only to Authorized individuals.

CONCLUSIONS

The adoption of electronic health records has been controversial and challenging in the US during last few years. In this paper authors have discussed the legal, privacy and security issues that arise with EHRs. Adopting best practices related to the privacy and security of healthcare data that are at rest are the pivot to the trust relationships needed when exchanging health data across the healthcare networks. Leaders in the healthcare practice need guidance for implementing the best privacy and security practices. Some of these best practices include understanding of the legal framework involved, managing information content and context, identifying and implementing appropriate technical solutions including the technical standards and architectures, and policy and procedural frameworks necessary to achieve secure and effective management of health information storage and exchange.

EHR systems are expensive, and the risks of privacy and security of patients' EHRs are great. However, it is certain that the use of EHRs would improve quality and efficiency of health care rendered to the patients. It is required that IT staff at medical facilities use network and data management best practices, follow risk assessment and management guidelines, and be on the forefront of technological advances to ensure the privacy and security of patients' data. If EHR and related technologies are implemented effectively, they can reduce medical errors, improve quality of patient care provided, and make healthcare more efficient.

REFERENCES

AMA – American Medical Association. (n.d.). Opinion 5.05 – Confidentiality. Retrieved from http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion505.page?

Appari, A., & Johnson, M. E. (2010). Information Security and Privacy in Healthcare: Current State of Research. *Int. J. Internet and Enterprise Management*, *6*(4), 279-314.

Babcock, P. (2005). National Plan for E-Health Records Gains Momentum. *HR Magazine*, August 2005, 29–32.

Carey, J., & Holahan, C. (2008). Google Goes to the Doctor's Office. *BusinessWeek Online*, 02/21/2008.

Centers for Medicare & Medicaid Services. (2014). Estimated Growth Rate and Conversion Factor, for Medicare Payments to Physicians in 2014. Retrieved from http://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/SustainableGRatesConFact/Downloads/sgr2014p.pdf.

Chellappa, R. K. (n.d.). Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security. Retrieved from http://www.bus.emory.edu/ram/papers/sec-priv.pdf.

Chor, B., Kushilevitz, E., Goldreich, O., & Sudan, M. (1998). Private Information Retrieval. *Journal of the ACM*, *45*(6), 965-981.

Clarke, I., Flaherty, T., Hollis, S., & Tomallo, M. (2009). Consumer Privacy Issues Associated with the Use of Electronic Health Records. *Academy of Health Care Management Journal*, *5*(2), 63-77.

Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2008). Watermarking and Steganography. London: Morgan Kaufmann.

DeNoon, D. J. (2008). Infant Mortality: U.S. Ranks 29th. Retrieved from http://www.webmd.com/parenting/baby/news/20081015/infant-mortality-us-ranks-29th.

EMR. (2005). Electronic Medical Records' Risks Feared. *The Information Management Journal*, *39*(9).

Evans, D. C., Nichol, W. P., & Perlin, J.B. (2006). Effect of the Implementation of an Enterprise-Wide Electronic Health Record on Productivity in the Veterans Health Administration. *Health Economics, Policy and Law*, *1*(2), 163-169. Cambridge University Press.

Fernandez-Aleman, J., Senor, I., Lozoya, P., & Toval, A. (2013). Security and Privacy in Electronic Health Records: A Systematic Literature Review. *Journal of Biomedical Informatics*, *46*(3), 541-562.

Fox, M. (2010). U.S. Scores Dead Last Again in Healthcare Study. Retrieved from http://abcnews.go.com/Health/HealthCare/wireStory?id=10987822

Gilbert, J. (2001). Privacy? Who Needs Privacy? *Business 2.0*, January 23, 2001, pp. 42.

Gulati, R. (1995). Does Familiarity Breed Trust? The Implications of Repeated Ties for Contractual Choice in Alliances. *Academy of Management Journal*, *38*(1), 85-112.

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Gunter, T. D., & Terry, N. P. (2005). The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions. *Journal of Medical Internet Research, 7*(1). Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1550638/.

Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., & Muller, G. (2011). Aspects of Privacy for Electronic Health Records. *International Journal of Medical Informatics, 80*(2), e26-e31.

Havenstein, H. (2005). Users Wary of Federal Medical Record Plans. *ComputerWorld*, *39*(24), 1-47.

Health Management Technology. (2008). Subcommittee Approves HIT Legislation. *Health Management Technology*, August 2008, pg. 9.

ISO 27001 Security. (2011). ISO 27799:2008 Health Informatics — Information Security Management in Health Using ISO/IEC 27002. Retrieved 1/12/2015 from http://www.iso27001security.com/html/27799.html

Kahn, S., & Sheshadri, V. (2008). Medical Record Privacy and Security in a Digital Environment. *IT Professional*, *10*(2), 46-52.

Kam, R. (2012). Top 3 Issues Facing Patient Privacy: Government Health IT. *Government Health IT*. Retrieved from http://www.govhealthit.com/news/top-3-issues-facing-patient-privacy

Keen, P., Balance, C., Chan, S., & Schrump, S. (2000). Electronic Commerce Relationships: Trust by Design. Englewood Cliffs, NJ: Prentice Hall.

Kimbuende, E., Ranji, U., Lundy, J., & Salganicoff, A. (2010). U.S. Health Care Costs. Menlo Park, CA: Kaiser Family Foundation. Online report, retrieved from www.kaiseredu.org/Issue-Modules/US-Health-Care-Costs/Background-Brief.aspx

Lohr, S. (2009). Digital Health Records: The Hard Road Ahead. *The New York Times*, 09/10/2009.

Martin, J. (1973). Security, Accuracy, and Privacy in Computer Systems. Englewood Cliffs, NJ: Prentice Hall.

Meeks, B. N. (2000). Is Privacy Possible in the Digital Age? *MSNBC*, 12/8/2000. Retrieved from http://www.msnbc.msn.com/id/3078854/.

Meingast, M., Roosta, T., & Sastry, S. (2006, August). Security and Privacy Issues with Health Care Information Technology. In *Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE*, 5453-5458.

Merisalo, L. (2012). Protecting Patient Privacy. *Healthcare Registration*, *21*(7), 5-9.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer Perceptions of Privacy and Security Risks for Online Shopping. *The Journal of Consumer Affairs*, *35*(1), 27-44.

Modern Healthcare (2009). Government Pumps Billions into IT. *Modern Healthcare, 39*(51), 26.

Mukherjee, A., & McGinnis, J. (2007). E-Healthcare: An Analysis of Key Themes in Research. *International Journal of Pharmaceutical and Healthcare Marketing*, *1*(4), 349-363.

National Health Expenditure Projections 2009-2019. Retrieved from http://www.cms.gov/NationalHealthExpendData/downloads/proj2009.pdf.

Palvia, P., Lowe, K., Nemati, H., & Jacks, T. (2012). Information Technology Issues in Healthcare: Hospital CEO and CIO Perspectives. *Communications of the Association for Information Systems*, *30*(19), 293-312.

Pear, R. (2010). Doctors and Hospitals Say Goals on Computerized Records are Unrealistic. *The New York Times*, 06/07/2010. Retrieved from http://www.nytimes.com/2010/06/08/health/policy/08health.html?nl=technology&emc=techupdateema3.

Porter, M. (2013). Adoption of Electronic Health Records in the United States. *Kaiser Permanente International*. Retrieved from http://xnet.kp.org/kpinternational/docs/Adoption%20of%20Electronic%20Health%20Records%20in%20the%20United%20States.pdf

Rothstein, M. A. (2007). Health Privacy in Electronic Age. *The Journal of Legal Medicine*, *28*(4), 487-501.

Stewart, K. A., & Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research, 13*(1), 36-49.

Udo, G. (2001). Privacy and Security Concerns as Major Barriers for E-commerce: A Survey Study. *Information Management & Computer Security*, *9*(4), 165-174.

Wang, H., Lee, M., & Wang, C. (1998). Consumer Privacy Concerns About Internet Marketing. *Communications of the ACM*, *41*(3), 63-70.

Westin, A. F. (1967). Privacy and Freedom. New York, NY: Atheneum.

Wilensky, G. R. (2014). Improving Value in Medicare with an SGR Fix. *The New England Journal of Medicine*, *370*(1), 1-3.

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy