Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2019 Proceedings | Southern (SAIS)

3-22-2019

Security and Privacy of Electronic Medical Records

Sajina Vinaykumar
Kennesaw State University, svinayku@students.kennesaw.edu

Chi Zhang
Kennesaw State University, czhang4@kennesaw.edu

Hossain Shahriar
Kennesaw State University, hshahria@kennesaw.edu

SECURING ELECTRONIC MEDICAL RECORDS: APPROACHES AND CHALLENGES

Sajina Vinaykumar
Kennesaw State University
svinayku@students.kennesaw.edu

Chi Zhang
Kennesaw State University
czhang4@kennesaw.edu

Hossain Shahriar
Kennesaw State University
hshahria@kennesaw.edu

ABSTRACT

Information Technology is being used in many ways to improve the quality and effectiveness of healthcare. Electronic Medical Record (EMR) is a medical record system that is computerized and delivers care in a healthcare institution. EMR tends to be a part of local stand-alone health information system that allows storage, retrieval, and modification of records. EMR are critical, highly sensitive, and private information in healthcare as the records are frequently shared among health care providers. The concern is about the security and privacy of health information on EMR; any person or party who provides, receives, manages or pays for healthcare. To ensure the security and privacy of EMR and protect them from cyberattack is essenital. In this paper, we perform a survey to identify tools, issues and challenges for securing EMR. We also discuss blockchain-based securing of EMR as well as overcoming known challenges and provide future direction of research.

Keywords

Electronic Medical Records (EMR), Electronic Health Records (EHR), Health Information System (HIS), Blockchain

INTRODUCTION

Information Technology is being used in many ways to improve the quality and effectiveness of healthcare. Patients, among all the stakeholders, have concerns and questions about the privacy and security of the health information on the Electronic Medical Records (EMR) Systems. Protecting the privacy and security of the EMR is essential. "The number of patient portals is rising, and although portals can have positive effects, their implementation has major impacts on the providing health care institutions" (Kooij and Groan et al. 2018).

As the adoption of EMR and EHR is increasing, in this study, we explored ten papers and found five prior research and tried to find out how to ensure the security and privacy of electronic medical records. We reviewed prior studies done in the past five years, from 2014 to 2018, from the US National Library of Medicine National Institutes of Health, PubMed.gov. The research methods used in the studies include qualitative and quantitative study. Information and data in these studies were collected through the research performed from selected interview, teledermatology, submitted research papers, online and onsite database searches, web-based surveys, questionnaires, pilot studies, journals, and articles. The interviewer in these studies worked with medical professionals, managers, and IT employees. The studies were conducted in different healthcare settings, such as cancer patient care, primary patient care, and various types of hospitals including university medical centers, teaching hospitals, and general hospitals. The research data included patient data stored in a local database management system in the hospital itself and on the cloud-based platform (Dubovitskaya and Xu et al. 2018). Data in these studies are organized based on the data category and encrypted with the corresponding patient key. The data collected through these studies were publicly available (Christiansen and Jur et al., 2017). The most commonly used database in healthcare is the online transaction processing database (Cardon, 2018). This healthcare database allows to replace the folders and replace the paper documents.

Based on the review of the prior studies, three critical areas discussed in this paper were; security and data protection, user support, and citizen adoption and use. The most frequently mentioned security measures and techniques in the prior studies are administrative, physical, and technical safeguards.

ISSUES AND SECURITY TECHNIQUES USED IN EMR

Sensitive information needs advanced security techniques. Most of the issues received are system functions, circulation, integrity, ease of use and continuity of the Personal Health Records (PHR), data security, and privacy protection. Security

measures and techniques are listed under administrative, physical, and technical safeguards. Legal and security challenges should be taken into consideration before using the shared electronic cooperation platforms and health record systems to avoid security threats during the implementation. It includes the allocation of responsibility, documentation routines, and integrated or federal access control (Christiansen et al., 2017).

One crucial element is eHealth literacy, that shares the information and evaluation strategies for using health technology tools. Studies have captured some features that older adults wanted for patient portal systems. While designing the future design process, the use of these systems by older adults should be taken into consideration. Personal health records provide awareness, and intention of health promotion. Health care delivery changes to patient-centered services, so PHR became an essential platform for consumers and providers. The government has introduced a web-based electronic medical records repository for consumers, not a PHR (Sakaguchi-Tang and Bosold et al., 2017).

Single Sign-On or SSO technology utilizes a badge reader placed at each workstation where clinicians swipe or "tap" their identification badges. SSO implementation reduces the time taken to log into various clinical software programs and in financial savings from moving to a thin client, which enables the replacement of traditional hard drive computer workstations. Health Information Management, or HIM, is increasingly becoming allied with the field of biomedical informatics, and both disciplines have common interests. Coding, privacy, and security of health information are necessary for the electronic exchange and secondary use of health information. Addressing issues in information governance is essential in the delivery of electronic health records (Nøhr and Parv et al., 2017).

Issues found in EMR	Issue Summary	References
System functions	Healthcare system functions include the service, service inputs, financing, and functioning.	[6, 13]
Circulation	Circulation connects the healthcare information systems and simplifies and improves patient care.	[5, 13]
Integrity	Integrity in healthcare means honest and trustworthy actions.	[6, 10, 13]
Ease of use and continuity of the Personal Health Records	Personal Health Records improves the quality of the healthcare, and it is easy to update the patient records in electronic form.	[2, 5, 10, 13]
Data Security	Data security in healthcare is a concern because it involves patient information and health records.	[5, 10, 11]
Privacy Protection	Privacy protection in healthcare includes protecting personal information and medical records.	[6, 8, 9, 11]

Table 1. Issues Found in EMR

Categories of Security Measures	Security Measures used in EMR
Administrative	eHealth Literacy
Physical	Single Sign-On or SSO
Technical Safeguards	Addressing issues in Information Governance

Table 2. Categories and Security Measures in EMR

BARRIERS AND FACILITATORS AFFECTING THE PATIENT PORTAL IMPLEMENTATION

From an organizational perspective, some barriers and facilitators are affecting patient portal implementation (Kooij et al., 2018). Patient portal implementation is a complicated process because it is not only a technical process but also affects the organization and its staff. Barriers and facilitators occurred at various levels and differed among hospital types (e.g., lack of accessibility) and stakeholder groups (e.g., sufficient resources) regarding several factors (Kooij et al., 2018). Effective communication between the healthcare professionals and patients is essential (Sakaguchi-Tang, et al., 2017). Their access to the information can contribute to this, and the patient portal facilitates communication between them. Technology is advancing, and cyber threats are also getting escalated. "The importance of storing such sensitive information has been emphasized to prevent personal information security problems, such as information leakage, hacking, tampering, and so on." (Kim and Cho et al. 2018).

The privacy and the security of the patient records is the most crucial barrier in the healthcare industry. There is a lack of resources in the technology area and financial difficulties, including the cost of training and support (Sakaguchi-Tang et al., 2017). There are similarities and differences between the hospital types and stakeholders, and managers and information technology employees. Similarities and differences include, documentation system, position, and the type of EHR systems, technology used in the hospitals. There is a barrier between access to technology and the ability to use technology and the internet. Legal issues and security challenges should be taken into consideration before using the shared electronic platforms and health record systems (Christiansen et al., 2017). The challenges are in the allocation of responsibility, documentation routines, and integrated or federated access control.

By looking at the facilitators, the evidence of the effectiveness of technology-related aspects on patient empowerment and health outcomes is an active facilitator. The other two facilitators were technical assistance and family, and provider advice (Bloomrosen and Berner et al., 2017).

BLOCKCHAIN FOR SECURING EHR

Blockchain-based Electronic Medical Records (EMR) information can benefit healthcare providers and physicians because of efficiency (Gue, 2017). This approach gives researchers access to broad and comprehensive data sets to advance the understanding of diseases, facilitate the development of new drugs, and enhance biomedical discovery.

EMR information can be managed by blockchain-base applications as EMR information is mostly standardized (Gue, 2017).With blockchain, healthcare activities, such diagnosis, blood work, and X-ray can be created as digital transactions that are then grouped into encrypted blocks with other transactions. Trusted individuates, such as administrators, physicians, and technicians, can access and validate transactions using access keys and then timestamp the transactions. Timestamps for validated blocks create sequences that show the order and procedure for every transaction. This approach improves the accuracy of patient records as transactions cannot be irreversible.

In the Electronic Medical Record (EMR) environment, it is important to establish trust and continued participation in health care organization (Azaria and Ekblaw et al. 2016). On patients' side, they don't need to doubt anymore confidentiality of their records and they can totally trust the decentralized record management system for managing their records. On researcher's side, the blockchain based EMR system can help scientists to keep track of the accuracy of data. Meanwhile, data on blockchain will be shared more easily.

Presently, healthcare organizations are trying to develop blockchain base platforms for cross-institutional sharing of EMR data. It has the potential to share data on blockchain instead of traditional way of requesting EHR data from different institutions (Peterson and Deeduvanu et al., 2016). However, there are still some problems in sharing data between organizations. When some organizations concern about privacy problems or commercial competitions, they might deny the access to share data from others. Different healthcare institutions sharing data require a standard data prototype. If one organization uploads data by different data types, and the other organizations cannot understand the data, it might cause errors in blockchain.

The problems of sharing healthcare data can be divided into three parts: (i) Security (ii) Infrastructure and (iii) Interoperability (Peterson et al., 2016). They are discussed below

Security: Security problem is one of the largest problems in data sharing currently not only in the healthcare emphasis. It might cause financial or legal consequences. There are two points to solve the security problem in blockchain based healthcare data sharing. First, each data sharing request must be processed between authorized access because an unauthorized address could expose the commercial advantage of organization or "reveal proprietary practices". The other point is to improve data anonymity of the user/organization in blockchain. This solution requires the user's information be separated from patient records for sharing before the information uploads to blockchain. And, developer can create an extra smart contract to include user's information.

Infrastructure: There are some infrastructure requirements during data sharing, which can be solved by increasing technical consistency of each block miner (data's owner/organization) in future. Data sharing between several organizations needs a centralized data source or "the transmission of bulk data to other institutions". However, centralized data source might request the trust of a single authority, which is the risk of security; and, bulk data transmission requires organizations to monitor, control and re-edit data during transfer data, which will increase quantity of work.

Interoperability: In the healthcare emphasis, the data is more complex due to large number of professional data/prototypes included. Therefore, when some non-healthcare background organizations request access of data sharing, interoperability of healthcare records is hard to solve. There are two types of problem in interoperability: data structure and semantics. Due high volume of professional knowledge included in healthcare data, data structure might be different from normal structures in organizations. Therefore, healthcare organizations need to create a standard data structure which non-healthcare organizations can be recognized and used directly. For semantics problems, healthcare organizations should create a professional digital dictionary or a smart contract for user, which can be called to translate those professional data to data which can be analyzed (Peterson et al., 2016).

There is decentralized record management system for Electronic Medicine Record – MedRec. MedRec uses blockchain technology (Azaria et al. 2016). The system allows patients to manage the log and access their data across providers and treatment sites. Base on the technology of blockchain, MedRec has an ability to improve authentication, confidentiality, accountability and data share. Those features are important for handling some sensitive information. The system encourages medical providers, researchers, public health authorities to be the "miner". The propose of this activity will give "miner" access to retrieve aggregate, anonymized data as rewards of mining in return for sustaining and securing the network via Proof of Work.

Factom is a software company that uses blockchain technology to store data on a decentralized system (Varshney, 2018). As a feature of Factom's technology, healthcare organizations can create smart contracts to develop medical data. The medical data needs to be encoded with a fingerprint of the data. Blockchain uses digital fingerprints to verify processes and time-stamping. Therefore, Factom technology can help healthcare organizations to protect patient's information confidentiality.

The decentralized management system MedRec records the relationship of patient and provider by smart contracts on Ethereum (Azaria et al. 2016). The system uses relationship smart contracts to check permissions and data retrieval instructions for external databases use. Under this foundation, providers can add a record for patients; patients can also access the sharing of records between providers.

Basically, the EHR system contains three types of smart contracts: Registrar Contract, Patient-Provider Relationship Contract, Summary Contract. Registrar Contract is used to identify the address of users (Azaria et al. 2016). Patient-Provider Relationship Contract is used between two nodes on blockchain which stores and manages medical records. Summary Contract is used for holding a list of references, which helps participants to locate their medical record histories.

FUTURE RESEARCH IDEAS

Future research can extend to other regions or remote areas and can use diversification methods for surveys. Study the long-term expansion of the program, the current study of the Self Adjusting File (SAF) system within the Epic EHR system limits by the long-term clinical outcome documentation, and small sample size (Carter et al., 2017). Among the empirical research papers, research on experts in information protection and medical personnel were the most common. The research should extend to different types of users.

Research can also include exploring scenarios such as connected health and medical data research and apply them in practice for the enhancement of current healthcare data management. Confirm the practical utility of the proposed model and find "satisfiers" determining the attitude of professionals toward using these technologies, which is important for the security of the patient health records in the hospital systems. Find the expectations before the implementation and the experience afterward among the healthcare professionals and patients. Expectation needs to be known to work towards the implementation of the systems and meet the expectation of the organization (Kooij et al., 2018).

Discuss leading issues in the association of HIM and informatics, examine the challenges, and provide the way for best practices. Understand and address the barriers to a patient portal, and ePHR use. Understand the changing technology in the design process for designing a flexible system that would ease future transitions from legacy systems. Study the patient portal experience among older adults from their use to adapt to the system (Sakaguchi-Tang et al., 2017).

Check the social perception and technology development to improve risk management in medical information systems. Further, check the firewall categories and cryptography methods identified, along with the other security measures in the healthcare

industry for the security of Electronic Health Records. Identify the legal and security challenges for further development, use of electronic collaboration, and documentation systems for integrated care (Kruse and Smith et al., 2017).

CONCLUSION

Information technology involves a risk of privacy violation as it provides easy access to confidential information through the internet. EMRs are critical and private information in healthcare and is shared among healthcare providers and patients. EMR allows modification, storage, and retrieval of records. Patients have concerns and questions about the security and privacy of their health information on the EMR. EMRs need to be protected from loss, hacking, and theft.

Areas	Area Summary	References
Security and Data Protection of Electronic Medical Records.	Electronic Medical Records are critical, highly Sensitive and Private information. Protecting the information is critical.	[6, 13, 11]
User Support in the use of Patient Portal and Implementation in Healthcare Institutions.	Patients should start using the Patient Portal for checking the health records in Healthcare.	[9, 14]
Citizen Adoption and Use of Electronic Medical Records.	Patients using electronic medical records in Healthcare.	[4, 9, 11]

Table 3. Areas Covered in this Paper

The information in Electronic Medical Records shared among the healthcare providers and patients through the internet. Information technology involves a risk of privacy violation as it provides easy access to confidential information including personal and medical information. Blockchain provides a unique opportunity to develop a secure and trustable EMR data management and sharing system. "In the case of a permissioned system, users do not have an incentive to cheat as their identity is revealed to the identity server" (Dubovitskaya et al. 2018).

Studies show the use of EMRs in different healthcare settings including cancer patient care, primary care, hospitals, and university medical centers. In EMR, eHealth literacy is necessary and teaches the evaluation strategies and information for health technology tools. Older adults wanted some specific features for the patient portal systems, and these should be included in the future design. Personal health records provide awareness, and intention of health promotion. PHR became an essential platform for consumers and providers because health care delivery changes towards patient-centered services. Single Sign-On implementation reduces the clinician's time spent logging into various clinical software and in financial savings from moving to a thin client. HIM is increasingly becoming allied with the field of biomedical informatics. Coding, privacy, and security of health information are necessary for the electronic exchange and secondary use of health information.

REFERENCES

1. Azaria, A. and Ekblaw, A. et al. (2016) MedRec: Using Blockchain for Medical Data Access and Permission Management, *MedRec.,* Retrieved February 10, 2019 from https://ieeexplore.ieee.org/abstract/document/7573685?reload=true
2. Bloomrosen, M. and Berner E. S. (2017) Findings from the 2017 Yearbook Section on Health Information Management, *Yearb Med Inform.*, 26, 1, 78-83, Retrieved June 3, 2018 from https://www.ncbi.nlm.nih.gov/pubmed/29063540
3. Cardon D. (2014). Database vs. Data Warehouse: A Comparative Review, Enterprise Data Warehouse/Data Operating System, *HealthCatalyst,* Retrieved February 10, 2019 from https://www.healthcatalyst.com/database-vs-data-warehouse-a-comparative-review
4. Carter, Z. A. and Goldman, S. et al. (2017) Creation of an Internal Teledermatology Store-and-Forward System in an Existing Electronic Health Record: A Pilot Study in a Safety-Net Public Health and Hospital System, *JAMA Dermatol,* 153, 7, 644-650, Retrieved June 3, 2018 from https://www.ncbi.nlm.nih.gov/pubmed/28423156
5. Christiansen, E. K. and Jur, C. et al. (2017) Shared Electronic Health Record Systems: Key Legal and Security Challenges, *J Diabetes Sci Technol.,* 11, 6, 1234-1239, Retrieved June 1, 2018 from

https://www.ncbi.nlm.nih.gov/pubmed/28560899

6. Dubovitskaya, A. MS. and Xu, Z. et al. (2018) Secure and Trustable Electronic Medical Records Sharing using Blockchain, *AMIA Annual Symposium Proceedings Archive*, 650-659, Retrieved June 1, 2018 from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977675/
7. Gue G. D'A. (2017) Why Blockchain offers a fresh approach to interoperability, *Health Data Management (Online)*, New York, Retrieved February 10, 2019 from https://www.healthdatamanagement.com/opinion/why-blockchain-offers-a-fresh-approach-to-interoperability
8. Kim, Y. W. and Cho, N. et al. (2018) Trends in Research on the Security of Medical Information in Korea: Focused on Information Privacy Security in Hospitals, *Healthc Inform Res.*, 24, 1, 61-68, Retrieved June 2, 2018 from https://www.ncbi.nlm.nih.gov/pubmed/29503754
9. Kooij, L. and Groen, W. G. et al. (2018) Barriers and Facilitators Affecting Patient Portal Implementation from an Organizational Perspective: Qualitative Study, *Journal of Medical Internet Research* 20(5), Retrieved June 2, 2018 from https://www.ncbi.nlm.nih.gov/pubmed/29752253
10. Kruse, C. S. and Smith, B. et al. (2017) Security Techniques for the Electronic Health Records, *J Med Syst.* 41, 8, 127, Retrieved June 4, 2018 from https://www.ncbi.nlm.nih.gov/pubmed/28733949
11. Nøhr, C. and Parv, L. et al. (2017) Nationwide citizen access to their health data: analysing and comparing experiences in Denmark, Estonia and Australia, *BMC Health Serv Res.* 17, 1, 534, Retrieved June 4, 2018 from https://www.ncbi.nlm.nih.gov/pubmed/28784173
12. Peterson, K. and Deeduvanu, R. et al. (2016) A Blockchain-Based Approach to Health Information Exchange Networks, White Paper, *Mayo Clinic*, Retrieved February 10, 2019 from https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf
13. Rau, H. H. and Wu, Y.S. et al. (2017) Importance-Performance Analysis of Personal Health Records in Taiwan: A Web-Based Survey, *J Med Internet Res.* 19, 4, Retrieved June 3, 2018 from https://www.ncbi.nlm.nih.gov/pubmed/28450273
14. Sakaguchi-Tang, D. K. and Bosold, A.L. et al. (2017) Patient Portal Use and Experience Among Older Adults: Systematic Review, *JMIR Med Inform.* 5, 4, Retrieved June 1, 2018 from https://www.ncbi.nlm.nih.gov/pubmed/29038093
15. Varshney, R. (2018) The non-financial side of Blockchain, Express Computer, Mumbai, Retrieved February 10, 2019 from https://www.expresscomputer.in/interviews/the-non-financial-side-of-blockchain/18813/