

Health Information System Security Privacy in View of Interoperability

James Ochieng Ogalo*

Department of Computing Science, Kisii University, School of Information Science and Technology, Kisumu, Kenya

ABSTRACT

Health records involve unique data which are highly subjected to privacy right security checks and its disclosure may lead to violation of this right and therefore cannot be implemented without additional consideration. The health care community has long recognized the potential for health information technology systems in its management, thus improving clinical and health care while reducing costs and this has synergized the access to health care services and information. The mobility in health care provision demands the need for sharing of patient data and this require interoperable health information Technology infrastructure, privacy and security of the resource and this will enhance stakeholders trust and promotes health information interoperability diffusion. It has been noted that the major challenge in the integration of Health Information Record Management system is interoperability and practitioners in a private practice may have difficulty obtaining complete information about a patient who is currently being hospitalized. The study established that interoperability and privacy issues still stands out as the major hindrance to sharing of health care records. There is a need for closer collaboration and trust between the major stakeholders in the industry focusing on their inclusivity in working toward the achievement of interoperability and privacy concerns.

Keywords: Health information system; Interoperability; Privacy rights; Information technology

INTRODUCTION

The information or data of patients held in a health Information system is so sensitive and its breaches contravene the privacy and confidentiality rights of an individual and therefore security is mandatory in the platform of exchange. The individual data asset ought to be protected by the hosting institution and it becomes there duty to ensure people's rights to consent, privacy, security and ownership around the information processes of collection, analysis, storage, presentation and reuse of data, while respecting the values of transparency and openness [1]. The health information exchange becomes paramount in the nature of patients mobility necessitating integrative needs of Electronic Health Record for accurate medical history and information needs for treatment at any instance and with entry of a particular patient number all the required details is made available and appropriate decision is made.

The health care community has long recognized the potential for health information technology systems electronic health records systems in particular to improve clinical care and health while reducing costs [2]. It is the mandate of the sector to bridge the gap that exist to achieve holistic information exchange from one point to the other and share data from the various existing devices to

deliver patient information for ease of handling.

In socio economic impact of m-health an assessment report of 2016, indicates that Digital Health could enable an additional 28.4 million people access to the healthcare system in Brazil, and an additional 15.5 million to the same in Mexico, without having to add a doctor. Total healthcare spend (public and private) could be reduced by \$14 billion USD in Brazil and \$3.8 billion USD in Mexico while providing the same care impact. This further improves the speed, accuracy and timeliness of information dissemination and uptake. Digital information technology has revolutionize all the corners of the global economy and has changed the way things are done and health care being a very critical area of concerns is no exceptional.

There are numerous impediments to data sharing that must be addressed by patients and organizations to facilitate effective traffic of Electronic health records. Interpreting the Health Insurance Portability and Accountability Act (HIPAA) has itself become a limiting factor for interoperability [2]. With the positivity results of Electronic Health Record, its data security and communication conformance is to be attained following the heterogeneity of the infrastructure. In securing eHealth Information, the Health Insurance Privacy and Accountability Act 5 Security Rule necessitates

Correspondence to: James Ochieng Ogalo, Department of Computing Science, Kisii University, School of Information Science and Technology, Kisumu, Kenya, E-mail: ogalojames@kisiiuniversity.ac.ke

Received: July 20, 2021, **Accepted:** August 03, 2021, **Published:** August 10, 2021

Citation: Ogalo JO (2021) Health Information System Security Privacy in View of Interoperability. J Pharma Care Health Sys. S7:236.

Copyright: © 2021 Ogalo JO. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

setting up of various safeguards including physical, administrative, and technical, to protect electronic health information. National Institute of Standards and Technology has been adopted [3].

Security issues come up when health information records are shared; this has to seek consent of the individual in question [4]. Health a record handling is unique compare to other sectoral records management, its disclosure may lead to serious violation of privacy rights issues and therefore cannot be implemented without additional consideration. The frequent eHealth information handling questions asked in this regard includes whom to share, how much to share, how to share in a way that no unauthorized can be made. This present a very serious security challenge solution based on the uniqueness and complexity of health information.

The essence of Privacy Rule is to protect individually identifiable information, mandating disclosure of what is perceived to be the “minimum necessary” and limiting disclosure of individual identified by the information; the entity’s own treatment, payment, and healthcare operations; uses and disclosures to which the individual has the option to agree or object; incidental use and disclosure; public interest and benefit activities; limited data sets which have been de-identified. Individuals have the right to view their data and amend it as needed; the right to be notified when and to whom individually identifiable data has been disclosed; and the right to request restricted access of their data to different entities [5].

In a study by KPMG indicates that the leading vulnerabilities in data security is sharing data between third parties and insiders (breaches by employees). Further the finding revealed that access control and authentication as key security features in eHealth infrastructures. Authentication being the initial stage of the users’ validation to determine their identity which is necessary to ensure that they are authorized to access the system [6]. The components ought to have ability to interpret and understand the data set coded in the communicating devices and provide results. In order to achieve interoperable health information Technology infrastructure privacy and security of the resource is a vital concern and in turns strengthen stakeholders trust and improves health information interoperability diffusion. There exist urgency for patients’ data and healthcare provision to be exchanged and shared through the Internet and the demand is on the increase from healthcare institutions and providers [7]. In the conceptual model identifies interoperability in three levels; Technical interoperability using standard communication protocols, Syntactic interoperability the sharing of the data information, Semantic interoperability dealing with the use of shared coding systems [8].

According to the Healthcare Information and Management Systems Society (HIMSS) 2005 technical interoperability is referred to as an enabled transfer of health data maintaining data integrity, safety, security, patient confidentiality and a common degree of quality of service.

Statement of the problem

It stands out that health information exchange from one point to another should be automated, shared and interpreted for utilization. Although this has been achieved to some extent there ought to be additional drive focusing on global wide interoperable health Information Technology infrastructure where all individual patients and their health care providers have a definite access to health information that provides informed decision-making, supports health management, allows patients active records to

be retrieved and exchanged amongst health and caregivers, and generally improves the overall health sector management and research.

The uptake of Electronic health Information exchange has been hindered by the risks of the information disclosure and identity theft, easy of manipulation of such records. However, the new technological advancement, the improved infrastructural framework, new options have been developed for incorporation and recent innovation for holistic exchange of health information but the entire process is still low. Therefore the study sought to review cases of interoperability and privacy rights in the diffusion of seamless electronic health records.

LITERATURE REVIEW

Data privacy and interoperability

The improved Interoperability rules is set to give new life in terms of data flows, and thus replaces some of the platforms discretion on data shared and further it comes with strings attached, in the form of legal obligations for informed consent and data minimization [9]. Asserts that in the implementation of electronic health records the ethical and legal aspect has to be taken into consideration in order to safeguard patient information. The mobility of people and divergence health issues require a one stop shop for the patient information and qualify the urgency of complete data exchange amongst health information devices and systems.

Interoperability process has been hindered by the legal, privacy and security issues. Wintry, doucette, daly, levy, and chrischilles, (2010) affirmed that concerns from providers in enhancing the interoperability of PHRs and Electronic Health Records (HER) have included issues of privacy and the accuracy of the information entered by patients. In addition, questions have risen as to whether the information entered by patients should be used to make medical decisions. Interoperability is defined as the ability of two or more systems or components to exchange information and to use the information that has been exchanged [10].

The drive to achieve the interoperability in healthcare is to facilitate the seamless exchange of health-related information amongst caregivers and patients for clinical decision making [11]. And this allows all patients, their families, and care providers able to send, receive, find, and use health information in a manner that is appropriate, secure, timely, and reliable.

Affirmed that the main challenge of Electronic Health Records Management is the integration, intraoperability and interoperability of various systems between various departments and users who may lack the understanding and knowledge of current information [9]. By the development of an interoperable health Informational infrastructural systems provides the accurate, timely and consistent health data across stakeholders and practitioners.

For exchange and transmission of patient’s data from various devices and Health Information Systems, the data security and interoperability are key, as put by that interoperability will only be achieved if the receiving system and users properly understand the meaning of information they receive and they are able to use this information [12].

It has been noted that the major challenge in the integration of Health Information Record Management system is interoperability and practitioners in a private practice may have difficulty obtaining complete information about a patient who is currently being

hospitalized; also a practitioner may repeat tests and procedures because he or she does not have prior information about the patient [11].

The achievement of interoperability in health sector is unique compared to the other sectors. The information in the healthcare domain is enormously complex, because it covers different types of data such as patient administration, organizational information, clinical data and laboratory/pathology data and it should be a one stop shop for health IT stakeholders, clinicians, hospitals, public health, technology developers, payers, researchers, policymakers, individuals and others for the integral development of Electronic Health Record [13].

Affirmed that large number of physicians in individual or small group practices with very limited administrative support for Information Technology and related practice changes; the lack of uniformity and interoperability of Information Technology systems from different vendors; regulatory limitations on hospital funding of Information Technology for physicians; lack of trust and other legal concerns with respect to joint Information Technology solutions; and privacy and security concerns as an impediment in the achievement of electronic transfer in health sector compared to other sectors like banks [14]. The data received from the various systems regarding the health information of the patient can be consolidated to trigger clinical decision and initiate accurate action by the caregiver or professional. The recipient system would take the data gathered from the various other systems and trigger clinical decision support, offering the provider suggestions for care actions.

Usability of health information systems

According to usability refers to how useful, usable, and satisfying a system is for the intended users to accomplish goals by performing certain sequences of tasks” (p. 1056). One of the hindrances to interoperability of electronic healthcare systems is the problem of usability amongst stakeholders in the circle of care [11,15].

The meaningful exchange of health related information amongst electronic healthcare systems is usability problem [16] noted that usability of healthcare Information Technology has continued to be a worldwide issue, with continued reports of systems that are unusable, negatively affect healthcare workflow, and might even introduce a new class of error-technology-induced error [17]. Reaffirmed that developed system should minimize memory load by making sure that users are not overwhelmed by what they see and how they interact with the system thus improving on density, poor end-user feedback [17].

Security of health electronic records

Designating user privileges is a critical aspect of medical record security: all users have access to the information they need to fulfill their roles and responsibilities, and they must know that they are accountable for use or misuse of the information they view and change [18]. Various security controls needs to be in place to provide security to the high complexity of eHealth systems. Audit trails track all system activity, generating date and time stamps for entries; detailed listings of what was viewed, for how long, and by whom; and logs of all modifications to electronic health records.

Silva et al., (2012) reaffirmed that health data ought to be permanently available, reliable and at high performance and in many healthcare units, fault tolerant systems are used, this ensure the availability, reliability and disaster recovery of data. However, these mechanisms do not allow the prediction or prevention of

faults. In this context, the necessity of developing a fault forecasting system emerges. It is necessary to monitor database performance to verify the normal workload and adapt a forecasting model used in medicine into the database context. Based on percentiles a scale to represent the severity of situations was created.

As much as the shift towards patient centered interoperability is a boost in the healthcare records management this also has its challenges ranging from security and privacy, technology, incentives, to governance that must be addressed for this type of data sharing to succeed at scale, and many of these challenges are still not solved for traditional interoperability [19]. Confidentiality, privacy, integrity, and contractual rights are enabled through strong cryptographic techniques including hash codes, and public and private keys [20].

Interoperability in health electronic records

The uptake of interoperability in healthcare has risen in the recent past and still more effort needs to be injected to achieve the degree of success it deserves. The milestone achieved so far includes; the use of standards, archetypes, web services, healthcare service bus, and interface engines and ontologies. In semantic health report (2009) affirmed that, in spite of these diverse solutions, interoperability within the healthcare domain is yet to be completely achieved [21].

The need to share health records both heterogeneous and homogenous systems are vital because of the mobility nature and the needs of patient from one location to another. The notable and the biggest obstacle facing Electronic Health Records interoperability are not technological but cultural. As in other industries, interoperability in health care requires the close coordination and collaboration of various stakeholders, including patients, providers, software vendors, legislators, and health information technology professionals. The records complexity and heterogeneity of the industrial players in healthcare cannot be compared to other industries like banking which have achieved major strides in the buildup of sharing and communications within them [14].

The major hindrance to interoperability issues are both providers and vendors who have been accused of “information blocking” or intentionally interfering with the flow of information between different Electronic Health Record systems [22]. Therefore complete interoperability and acceptable security of sharable electronic health records have to be sought; Integrating the attributes defined in multiple systems often result in semantic differences leading to partial mapping of data; identifying commonalities of meaning and usage of conflicting terms in health data is impossible without user intervention; The semantic differences in attributes need to be identified with the help of reasoning rules that would form the basis for logically establishing similarities between them; to search for a global optimal solution that best suites the ontology constraints can be best achieved through exploration of non-instance based learning approach. Ontology mapping relies heavily on features of its concepts definitions and explicit semantics of these definitions; Understanding and interpreting medical terminologies correctly is a bigger challenge [23-26].

Semantic and syntactic interoperability

The main goal of interoperability in healthcare is to connect applications and data, so that they can be shared throughout the environment and distributed by health professionals. In this way, the information is always available and accessible in order to make health professionals’ workflow [27].

For the achievement of interoperability in the healthcare there ought to be proper understanding of the meaning of information received both from the users and the receivers [12]. Semantic Interoperability lies at the top of the communications pyramid and in the setting of healthcare, semantic interoperability is critical for bridging the terminology gap among divergent Health Information Technology systems and data sources. Semantic interoperability takes advantage of both the structuring of the data exchange and the codification of the data including vocabulary so that the receiving information technology systems can interpret the data.

This level of interoperability is possible *via* potentially disparate Electronic Health Record systems, business-related information systems, medical devices, mobile technologies, and other systems to improve wellness, as well as the quality, safety, cost-effectiveness, and access to healthcare delivery [28]. Syntactic interoperability allows two or more systems to communicate and exchange data; however, the interface and programming languages are different. It allows the exchange of information among different systems or applications through a grammar. The entity that sends the information encodes it, respecting the syntactic rules of a specific grammar. On the other hand, the entity that receives the information decodes it using the same syntax rules.

Futures of health electronic records

Block chain technology has the capability and the role in improving interoperability in health data given its emphasis on sharing, distribution, and encryption. The newer block chain efforts of smart contracts, second-layer systems, and permissioned block chains further improves its potential in health care use-cases, and there has been no shortage of hype surrounding the potential of the technology within healthcare [29]. The Information Communication Technology enabled solutions supports the provision of effective, efficient, good quality, seamless healthcare are an old dream, this has been conceived about 40 years ago, but the large scale implementation has not been successfully achieve and the progression is ongoing.

The funding for the infrastructural development of eHealth raises a lot of question and in reported that European investment levels in healthcare ICT have remained almost static at around 1% to 1.5% of total healthcare expenditure. But now, a new set of common political imperatives is driving demands for additional funding to establish effective healthcare ICT infrastructures: pressure to secure acceptable levels of patient safety, expectation of 'consumer-type' access to health services, need for radical improvements in service productivity and impact of increasing complexity of healthcare processes [30].

At present to some extent, the healthcare system is characterized by increased costs, high error rate, and knowledge mismanagement and this could result in high rate of mortality and with the exchange and communication across the information technology infrastructure could significantly reduce and the lack of interoperability amongst healthcare systems further strengthens the information silos that exist in today's paper-based medical files, which results in proprietary control over health information. This has resulted in increased healthcare cost, declining quality of patients care, and the inability to integrate patients' information across healthcare systems. Moving forward integration of block chain technology in the design of healthcare data management would fix the dilemma of systems communication and data sharing and moreso, it is very

important to understand upfront what compliance requirements are applicable. These can be predicated on data type and sensitivity intended for storage on the block chain, the deployment architecture of the block chain network, and where block chain nodes are physically located. [31].

DISCUSSIONS OF FINDINGS

Health records involves huge volume of data sets and require analytical data mining to generate information relation to diagnosis, testing, monitoring, treatment and health management of patients, billing for healthcare services and asset-management of healthcare resources [32]. This require high powered combination of artificial intelligence, cloud computing and big data analytics, which has the potential of holding and manipulating huge of data for healthcare and thus improve the lives of millions of patients worldwide with better diagnostics, personalized treatments, and early disease prevention [33]. A great deal of how we organize healthcare is predicated on the 'ownership' of information, and controlling it's distribution and making high quality coded data available through secure, real-time APIs as well as by documents and messaging paradigms, and be able to share information in a way that the recipient can understand what we are saying, bridging the gap of semantic interoperability.

Healthcare integrated system require ability of machines to communicate efficiently, regardless of make or the institution where they reside, offering a vital health benefit, data become exceptionally mobile. Personal health information, entered into a system once, becomes available to patients wherever they are and whenever they need it. Data integrity, privacy and security are key in standardizing interoperable platform for capturing, storing and transmission of data. This has been a problem over the years [34-36]. Categorizes this standards into three levels; classification, vocabulary, and terminology standards; data interchange standards; and health record content standards.

CONCLUSION AND RECOMMENDATIONS

In the recent times the newest interoperability innovation platform formulation is an inevitable and seamless exchange is designed to reduce the burden of data curation, making usable information forefront in enhancing patient care. Digitization of health sector is dependent on interoperability and standardization of data and in achieving secure interoperable infrastructure in e-Health require a more dynamic tactic with unique and appropriate security method to safeguard different domain. Need for closer collaboration and trust between the major stakeholders in the industry focusing on their inclusivity in working toward the achievement of interoperability. The block chain technology adoption and diffusion is major strait to bridge the sectors issues centered on privacy and security of information and set to improve data exchange and trust for patient driven interoperability.

In the usability context the industrial players should invest in system design and usability evaluation to improve the user appreciation of the functionality of the interoperable systems. Integrative policies on collaboration and information sharing embraced by all stakeholders focusing on innovative solution in bridging the gap of information sharing in healthcare systems ought to be formulated with enforceable legal regulation.

Various stakeholders' interest come into play and doesn't work well for the achievement of interoperability gap in healthcare. Solid

policies which embraced by all the also requires policies that provide incentives for interoperable data exchange and, if necessary, enforce interoperability *via* legal regulations. The strategies of streamlining communication and coordination with other players across all networks. The improved functionality of health information to be available to other providers.

REFERENCES

1. Responsible Data Forum. In: The hand-book of the modern development specialist: Being a complete illustrated guide to responsible data usage, manners and general department, responsible data forum. 2016.
2. Washington DC. ONC: 2016 Interoperability Standards Advisory (Best available standards and implementation specifications. 2015.
3. NIST Guide for mapping types of information and information systems to security categories. NIST 1-59. 2010.
4. Ozair FF, Jamshed N, Sharma A, Aggarwal P. Ethical issues in electronic health records: A general overview. *Perspec Clinical Res* 2015;6:73-76.
5. HIPAA Privacy Rule. Office for civil rights, US Department of health and human services.2013.
6. KPMG. Health care and cyber security: Increasing threats require increased capabilities. 2015.
7. Dwyer D, H Liu. The impact of consumer health information on the demand for health services. *Q Rev Econ Finance* 2013;53: 1-11.
8. Tolk A, Muguira JA. The levels of conceptual interoperability model, Fall SIW SISO 2003.
9. Quek KF, MZain AZ. Implementation and issues concerning electronic healthcare records. *J Healthc Commun* 2016;1: 3.
10. IEEE Standard Computer Dictionary. A compilation of iee standard computer glossar-ies IEEEStd. 2000;610.
11. Iroju O, Soriyana, Gambo I, Olaleke J. Interoperability in healthcare: Benefits, challenges and resolutions. *IJIAS* 2013;3: 262-270.
12. Transatlantic Consumer Dialogue. Resolution on Software Interoperability and Open Standards. 2008; 1-6.
13. Ryan A. Towards semantic interoperability in healthcare: Ontology mapping from snomed-ct to HL7 version 3. *CRPIT* 2006;72: 1-6.
14. Rosati K, Lamar M. The quest for interoperable electronic health records: A guide to legal issues in establishing health information networks. *AHLA* 2005;1-107.
15. Zhang J, Walji M. TURF: Toward a unified framework of EHR usability. *J Biomed Infor* 2011;44:1056-1067.
16. Kushniruk A, Nohr C, Jensen S, Borycki EM. From usability testing to clinical simulations: Bringing context into the design and evaluation of usable and safe health information technologies. *Yearb Med Inform* 2013;22: 78-85.
17. Boone E. EMR usability: Bridging the gap between nurse and computer. *Nursing Management* 2010;41: 14-16.
18. American Health Information Management Association (AHIMA). The 10 security domains (updated). *J Am Health Inf Management Assoc* 2012;83:50.
19. Julia Adler-Milstein. Moving past the EHR interoperability blame game. *N Engl J Catal* nd 2018
20. Suberg W, Alibaba. Deploys blockchain to secure health data in Chinese first. *Cointelegraph*. 2017.
21. Semantic Health Report. Semantic Interoperability for Better Health and Safer Healthcare. *EU Info Soc Med* 2009;1-34.
22. Nationwide interoperability roadmap. Office of the national coordinator for health information technology. Connecting health and care for the nation: The 2015 nationwide interoperability roadmap. 2015
23. Harvey F, Kuhn W, Pundt H, Bishr Y, Riedemann C. Semantic nteroperability: A central issue for sharing geographic information. *Ann Reg Sci* 1999;33:213-223.
24. Dolin RH, Alschuler L. Approaching semantic interoperability in Health Level Seven, *J Am Med Inform Assoc* 2011;18:99-103.
25. Kalfoglou Y, Schorlemmer M. IF-Map: An ontology-mapping method based on information-flow theory, S. Spaccapietra et al. (Eds.). *J Data Semant* 2003;98-127.
26. Bhartiya S, Mehrotra D. Threats and challenges to security of electronic health records. In *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*. *SJR LNICST* 2013;115:543-559.
27. Rogers R, Peres Y, Müller W. Living longer independently-a healthcare interoperability perspective. *EI* 2010;206-211.
28. eHealth Stakeholder Group report. Perspectives and recommendations on interoperability. 2014.
29. Gordon WJ, Wright A, Landman A. Blockchain technology in health care: Decoding the hype *NEJM Catal* 2017.
30. Frost and Sullivan. European electronic medical records markets.2013.
31. Alferes JJ Bertossi L, Governatori G, Fodor P, Roman D. Rule technologies. research, tools, and applications. *Stony Brook (NY): 10th International Symposium, Rule ML* 2016;6-9.
32. Bock C, Carnahan L, Fenves S, Gruninger M, Kashyap V. Healthcare strategic focus area: Clinical informatics. *National institute of standards and technology, technology administration, department of commerce, United States of America*. 2005;1: 1-33.
33. Jensen PB, Jensen LJ, Brunak S. Mining electronic health records: Towards better research applications and clinical care. *Nat Rev Genet* 2012;13:395-405.
34. Wager K, Lee F, Glaser J. *Health care information systems: A practical approach for health care management*. Jossey-Bass, San Francisco. 2009
35. Witry M, Doucette W, Daly J, Levy B, Chrischilles E. Family physician perceptions of personal health records. *Perspective AHIMA*. 2010.
36. The European EMR market is currently worth €349.6m and will reach €1.15bn by 2013.