International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206441

Electronic Medical Record and Security Concerns

Nkem D. Obaloje, Monday O. Eze
Department of Computer Science, Babcock University, Illishan-Remo, Nigeria

Article Info
Volume 6, Issue 4
Page Number: 235-246
Publication Issue :
July-August-2020

Article History
Accepted : 20 July 2020
Published : 27 July 2020

ABSTRACT

A number of critical questions remain unanswered in Health-care organizations, which are key to tactical planning, remaining competitive, among other issues that seek for answers from the information technologies spheres. Numerous establishments are evolving to fuse clinical computer unit, which dispense a solitary point of entry for permission to administrative, patient-related and research information. The medical record in a new embodiment lies at the center of developing clinical computer unit: accessible, protected, confidential, acceptable to patients and clinicians; fused with other, non-patient information that are specific. This study presented a review of Electronic Medical Record (EMR), security concerns and security frameworks proposed to improve the security concerns of EMRs. This study was able to provide an insight into the security concerns of EMRs, as well as, the barriers in use and adoption of EMR by health institutions which will bring about improved health services, especially in developing countries where manual record system are still prominent.

Keywords : Security concerns, Electronic Medical Record, Use and Adoption

I. INTRODUCTION

The creation, gathering, management of health records of an individual of authorized staff within one health maintenance institution that is electronic is termed Electronic Medical Records. Noteworthy gains can be attained by health institutions, physicians through EMR. EHR is often mistaken and confused with EMR. An extensive, elaborative, all inclusive medical history of an individual that showcases more functions in comparison to EMR is what EHR stands for (Lynn, Joy, & Rogers, 2017).

There is an urgent obligation for data to direct policy making, action strategies, planning and efficient care of health zones and health facilities to ensure the delivery of quality health service and patient access equity (Nzioka *et al.*, 2010). Cowie, Curtis, & Blosmster., (2016) affirms that the major aspiration of medical documentation is to ease Clinical investigation and serve as storehouse for what has been noted and or analyzed by the Clinician from the patient's information. Different clinicians make valid input on a particular record such as results from a test (x-ray or laboratory) and data from the administrative pool. From time to time, a variety of records are usually cared-for in diverse places. Several elements of the records are often stashed in various outlets. They can also be used as a medium of

communication among different clinicians as well as ancillary professionals (such as respiratory therapists, nurses, physical therapists) who gives audience to the patient. In the event of claims, medical documentation serves as a valid record due to occupational injury or wrong doing.

In recent years, the charge and quality of medical care has been of great interest. EMR suffices as the benchmark for quality satisfaction by companies, health care parastatals that handle insurance maters, the federal government and a host of others. Decision support in contemporary times has been an additional section of use. Potential drug interactions pose a great threat and therefore clinicians are been drawn to the need for test because of its effectiveness. Lynn, Joy, & Rogers, 2017 affirms that all these current plans are made possible by EMR. The private and public sectors have questioned the data and information been used from the EMR for some time now. This was due in part to the inadequate infrastructure of health information, a deficient information environment, quality management to support information gathering, delivery and data storage as well as security concerns (Nzioka *et al.*, 2010). A standard health record network is shown in Figure 1.

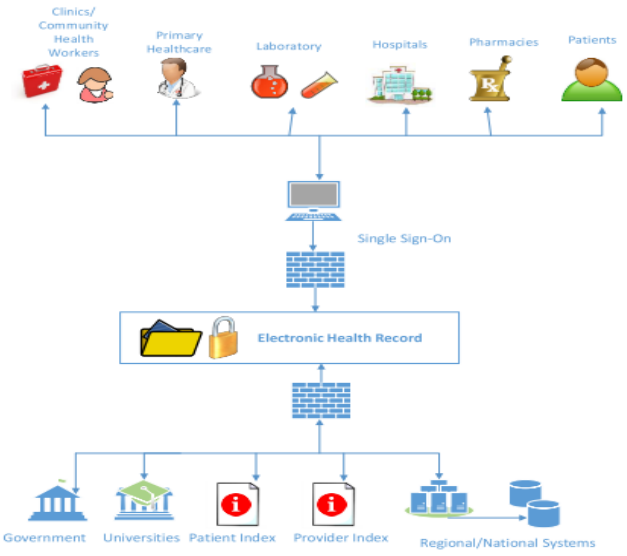

Figure 1 : The Electronic Health Record Network
Source: (Senese, 2015)

1.1 A Distributed Electronic Medical Record

Dependency on paper in most hospitals is prevalent. They may attend to hundreds of patients daily. The pile of paper work daily makes it almost impossible for the staff to debrief all the records because of the heap in the store room. The ability to coordinate and share information across several sites which would fast track entry to information been required is called a distributed operation. The ability for details to be distributed from a central open EMR server to other EMR guests which might be archaic clinics or hospitals is made possible by a distributed electronic medical record as seen in Figure 2. Lapses seen in other systems are gotten rid of by a distributed electronic medical system.

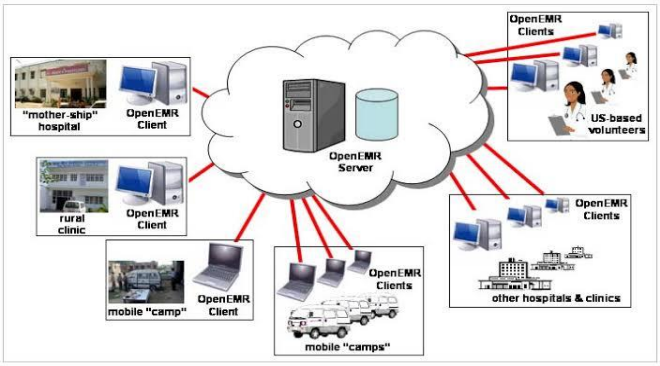

Figure 2 : An Electronic Medical Record System block diagram been distributed.
Source: (Randy, 2008)

1.2 Role of Electronic Medical Records System

The purpose of recording patient information was the reason why EMR systems evolved. Lynn, Joy, & Rogers, 2017 pointed out six functional areas EMR systems must deal with. These areas adhere strictly to the EMR Standard and Guidelines.

1. **To provide and document clinical health details and fundamental demographic**. This contains patient's identification number and pertains to information that is patient related and data of the patient when they meet.

2. To allot a clinical decision support. Abnormal vital signs, abnormal test results are meant to pop-up as notifications on the EMR systems so as to keep the providers of any impending danger. If a known allergic drug is prescribed or if a known drug interaction is likely to occur; reminders of recommended care due such as tests and medication due are provided.

3. **To provide order entry and prescribing**. A process whereby a healthcare worker electronically delivers instruction for the treatment and possible care of patients under his observation is called order entry.

4. To provide health information and reporting. Reports are generated by EMR systems from clinical data that reinforces quality advancement and produces reports that are aggregate.

5. Security Support and Confidentiality is Provided. Confidentiality and Health data security is the basis to any EMR system to guarantee patients data and their privacy is sustained.

6. **Makes the exchange of electronic information easy**. EMR systems are obligated to promote inter-operability among systems which would enable it to receive patient information, give rise to aggregate clinical care information and generate patient summary details using a standard; acceptable across board.

1.3 A Ranking of Health Record

When a patient's record stating his /her health data is well separated into different categories, it is called A Hierarchical Health Record. It aims at encrypting patients records in several sections according to hierarchy which is displayed in Figure 3. When a psychiatrist gains entry to a patient's health records, the clearance given to him/ her permits to view the patient's mental records and thereby, guarantee privacy of medical records stored electronically.

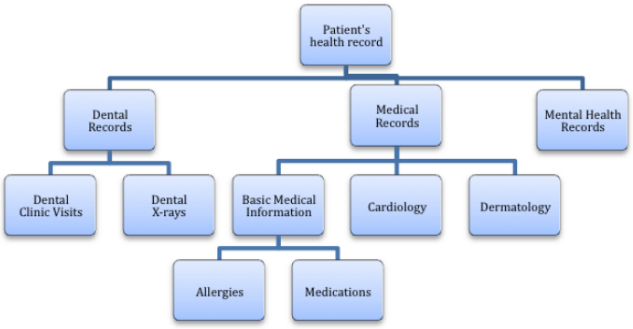

Figure 3: A Ranking of Health Record

Source: (Josh, Melissa, Eric, & Kristin, 2009)

1.4 Gains of Electronic Medical Records

Noraziani, et al., 2013 affirms that Medical Records stored electronically offer patients more adaptable means of gaining access, gathering and preserving medical information. Key gains have also been stated out (Pamela, and Sandra, 2014).

1. Encourage Proactive Healthcare Practices: In identifying patients in need of specific services, an EMR system can fuse verified based advice for precautionary services.

2. Immense Checks and Balances: Entry to medical data at the point of care, compliant coding accurate multimedia corroboration, and when information is entered only once, it reduces the plausibility of making medical errors.

3. Reporting Capabilities Improved: Users are allowed to design reporting formats and model attestation geared towards the needs of patients in several ways to satisfy the patient's needs. These are made possible because of its flexible output formats. Other parties who require health information are not exempted.

4. Fulfill Patients' Satisfaction: Medical errors are minimized to the barest minimum which also enhances the quality received. The patient's feels gratified.

5. Support in Decision-Making: Prescription and Procedures are tracked thereby, providing best practices that rely on knowledge from clinical base systems.

1.5 Pros for Electronic Medical Records

Noraziani, et al., (2013) outlines the Characteristics of Electronic Medical Records which satiates the user's prospects as stated below:

1. **Safeguarding Information Confidentiality**: Provide records on clinical information alongside diagnostic process/ personal information that are sensitive as well as placement orders and plans of care.
2. **Possibility of Lost Records is minimized**: Other critical data alongside test results which are in their electronic form are saved on the server. This guarantees the safety of patient records.
3. **Improve Quality and Originality of Documentation**: Healthcare providers are striving to bring down to the barest minimum their dependency on records written by hand and execute systems that are far better; thereby, producing efficient storage of patient interactivity.
4. **Service provided is enhanced**: Waiting time is minimized with easier and faster rate of progress which improves workflow efficacy and productivity in organizations.
5. **Improve Communication Between Providers**: Improves interdepartmental communication; giving room to numerous entries to documents at a single time. The communication between various departments in an organization is fused.
6. **Information is Accessible**: When information is needed at any department, it is easily accessed. A high percentage of access to information improves patients care by the provider.
7. **Medical Data Linkage**: Decision support system can be linked to electronic data. Therefore care plans, pharmaceutical information, clinician to protocols, databases of literature, critical paths and other databases with knowledge on healthcare can be linked to the EMR.
8. **Cost Savings**: A decline in inefficacies experienced in work places become evident. Medical records stored electronically to a large extent saves cost..
9. **Data Storage is enhanced**: Physical storage space by far outweighs the space stored on digital computers. Keeping of large paper works becomes a thing of the past.

1.6 Cons of Electronic Medical Records

Highlighted below by Noraziani, et al., (2013) are cons of the Electronic Medical Records. They are not bounded to the following:

1. **Cost of Acceptance is High**: When it comes to the implementation of EMR's, cost effective services are scarce.
2. **Limitation on Interoperability**: Technical specifications that enable interoperability when data is been exchanged between distributors who use different health IT systems are very scanty in number.
3. **Lead to Medical Error**: Relying solely on EMR by Healthcare personnel should be discouraged when it comes to plan that has to do with care management.
4. **Require Comprehensive Personnel Training**: EMR implementation requires personnel to be taught when it comes to the utilization of computers.
5. **Standardization of Documentation Systems is absent**: Variation into documentation in systems which lead to forms of document not up to standard is due to different system software in the market.
6. **Threats make EMR vulnerable**: Threats are also gaining ground with the enlargement in information technology such ignorance, inadequate behaviour, recklessness, curiosity, viruses, hackers, alongside spyware attacks and invaders in the environ.

1.7 Use and Adoption Concerns of Electronic Medical Records

A number of barricades arise from the adoption of EMR. The barriers are fundamentally in line with results of the study conducted by Ajami, and BagheriTadi., (2013); NasserH.Zaied, Elmogy, and

Abd Elkader., (2015) and McDermott, Kamerer and Birk (2019). Challenges observed are further classified into the following groups:

1. **Time:** Medical professionals refuse to create time to get acquainted with the accessible technologies properly, adopt it and learn to use it. This could be as a result of not having enough time needed to participate in full training on the use of EMR and learning new features.
2. **Lack of Technical Ability:** As a result of not creating time to learn the use of EMR, many physicians tend to lack the required technical ability. The expertise required to respond to patient concerns, evaluate medical significance, consider treatments and even form notes include a considerable degree of focus, typing abilities and experience with the user interface of the program.
3. **Password distribution:** The distribution of credentials presents a challenge to EMR personal privacy and repudiation.
4. **Typographic Errors:** This is a hazard to EHR precision and performance. Healthcare business is strongly aware of mistakes and quality is of prime concern here. Typographic errors are widespread danger primarily because of the lack of professional expertise inherent in data entry operators.
5. **Cost of implementing EMR:** Due to the cost of implementing a standard EMR, physicians also need to weigh available options; thus, contravening the EMR's advantages. Costs are the greatest deterrent to growth for small and medium-sized companies with no broad IT budgets. This is exacerbated by confusion about the scale of any financial benefits that can accrue over time.
6. **Security and Privacy: Fears Arising:** Notwithstanding facts to the opposite, non-users agree that EMRs pose greater protection and confidentiality threats than paper records and this could result in reluctance in adopting EMRs.
7. **Doctor-patient interaction:** A few scholars have discussed the capacity for problems of contact between doctors and patients while utilizing EMRs. The patient's eye interaction is and thus the more comprehensive, the better direct connection, which may contribute to better quality treatment.
8. **Navigation Intricacy**: The various displays, choices, and EMR accessibility navigational assist problems particularly for tracking advancement jottings cause physicians to expend additional work time studying efficient channels to use the EMR. Such large cost spent on time are obstacles to obtaining advantages, since higher demands on general practitioners resources limit usage of EMRs, thus growing capacity for increasing efficiency.
9. **Lack of technical Support**: Technical support encouraged usage of the EMR at any time. Support services were usually viewed as competent and supportive, although some doctors noticed that support workers were often inaccessible due to holidays and off work hours.
10. **Interoperability:** Interoperability as a driving factor in the implementation could minimize and promote the diffusion and transfer of new medical information by doctors. Interoperability significance is of no match as it reduces the expense of electronic health records and allows for possible single/ limited number of doctors to obtain thereby implementing such programs.
11. **Concerns about Data Entry**: Practicing family medicine needs a range of expertise, a fast rate, handling multi-age individuals, diagnosing symptoms from a multitude of often different concerns, and keeping a detailed database from various sources. Such considerations make data collection the biggest possible impediment to the successful usage of machines in family medicine.
12. **Data Exchange is Insufficient**: The scarcity of adequate electronic data trade-off between the EMR and other clinical data systems, restricts

workflow, takes unnecessary time to manually input records from other programs, and grows non-compliance among physicians to use EMR.

13. **Integration with other Health Institutions**: Doctors were reluctant to use medical records from EMRs to which they had little exposure, but needed to focus on written documentation instead. As an obstacle to "seamless entry" doctors described needing to sign in separately to inpatient and outpatient EMR systems.
14. **Timely-Availability of Data:** The physicians will not acknowledge the loss of accuracy of health data through network changes or power outage. The interests in the healthcare sector cannot tolerate any disruption whatever the least.

2.0 Security Concerns and Issues in Electronic Medical Records

The errors resulting due to the usage and implementation of EMR's are of immense concern and they have increased. A number of actions have been taken to assimilate the security concerns and issues. Dealings between people, environment and the nitty-gritty of technologies, tasks, and organisation where they function have been the cause for the emergence of security concerns. It suffices to ensure the utilization of EMR is well secured; thus, providing further knowledge into secure implementation of EMR which should serve as a tool for the advancement of the emotional and physical wellbeing and protection of patients. The absorption of EMR has drawn focus to threats and issues surrounding privacy in Healthcare organisations. Infraction in privacy in affiliation with data of medical origin remain as topic for discussion in the broadcasting industry, giving serious insinuations for users of healthcare and their patients. False entry into data have ways of denting the reputation of healthcare organisation's. Capable civil and criminal liabilities as well as monetary fines follows suit. Abdul-Rahim, Ismail, Salahuddin, & Samy., (2016) affirms that basically, health care parastatals' duty makes sure their healthcare employees regulate and handle EMR just the right way with adequate security measures.

The EMR systems should have intrinsic security control measures which include; Access Control, Secure information in transit and storage, Audit Trails, and Backup procedure (Nzioka *et al.*, 2010).

1. **Access Control:** This is a mechanism that controls the entry alongside the utilization of the EMR system. Access and use of the record can be in part or its entirety, however, the access is based on some assigned and predetermined role, responsibility, functions to be performed. Such as read only, editing, saving, or deleting patient's records. In identifying what access to give to the EMR user, the system should be able to authenticate and identify the user before he/she is able to perform any function on the system.
2. **Secure Information:** This is a mechanism for securing the patients data from being utilized by unauthorized user by using cryptographic techniques. This involves the use of cryptography such as symmetric, asymmetric and hybrid encryption, to secure the patients data both in storage and in transit. Thus, securing the EMR from various cyber attacks while providing confidentiality, integrity, non-repudiation and availability.
3. **Audit Trail:** This is a mechanism that allows visibility on the sequence of execution of system functions and processes. Audit trails are to be logged as evidence of user transaction within the system. In audit logs, date and time of a particular event, identification of the user that performed, initiated or completed the event, type of event performed, status of the event, security events must also be logged.
4. **Backup:** This is a mechanism that ensures data are protected and secured in case of data damage or data loss. It is a procedure of ensuring duplicate

copies of data are available and can be retrieved when the need arises. It is best practice for backups not to be on the same location as the original data store. This procedure should be done automatically and regularly within the system to ensure consistency.

2.1 Existing Security frameworks for Electronic Medical Records

1. Liu and Park, (2012), proposed a security framework that addresses security concerns that arise during transmitting and processing EMRs, Personal Health Records (PHRs), and billing record. The framework which is shown in Figure 4 enables multi-party participation, end-to-end security control and variable visibility into selective part of data by employing a security protocol at the network layer. Thus, providing integrity checking, authentication, encryption and replay protection, while supporting interoperability and ensuring multiple party participation in a controllable manner.

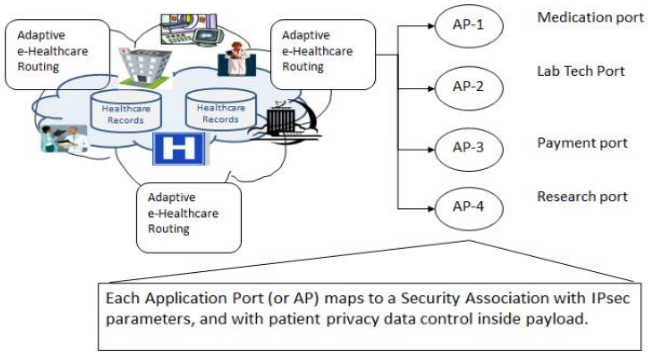

Figure 4: Security Framework proposed by Liu and Park.

Source: (Liu & Park, 2012)

2. Senese, (2015), proposed a security framework that utilized the Strawman Design access control mechanism, as shown in Figure 5. The Strawman approach incorporates the use of data store with different data option such as collection, preprocessing, insertion, and retention.

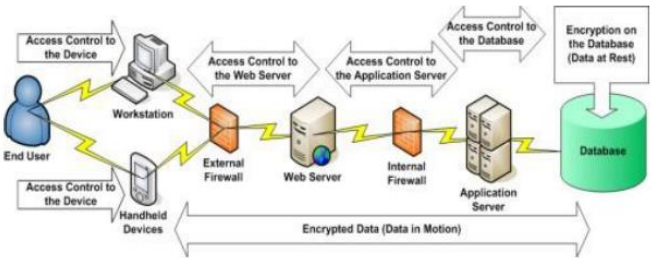

Figure 5: Framework proposed by Senese.

Source: (Senese, 2015)

3. Plachkinova, Alluhaidan, and Chatterjee, (2015), proposed a security framework for cloud based EMRs. This framework which is shown in Figure 6 consists of 5 phases which seem to represent a flow that can be applied during decision making as regards implementing EMRs. The first phase is referred to as the requirement phase. The second phase is the Service Level Agreement. The cloud implementation and evaluation are the third and fourth phase respectively while the monitoring and improvement are in the final phase.

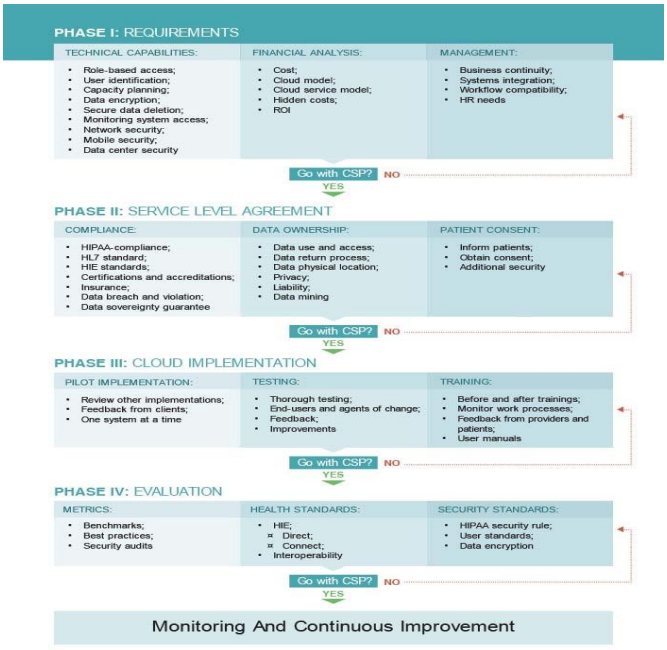

Figure 6: Security Framework for Cloud Based EMR proposed by Plachkinova, Alluhaidan, and Chatterjee

Source: (Plachkinova et al., 2015)

3.0 Literature Review

The focus of the literature review basically ascertains the various methods by which security concerns in Electronic Medical Records could be enhanced and

the techniques and instruments in existence provided. Various investigation also embrace the opinion that, the sudden embracement of EMRs and the urgency to distribute/share these data amongst patients and healthcare users, the assurance that the documentation are safe need to be functional for improved and adequate security of medical records. Frameworks of various origins have been proposed over time to drive home better security to Medical data stored electronically.

Josh, Eric, Melissa, & Kristin (2009) presupposed A Patient Controlled Encryption scheme that allows decryption keys to generate subkeys by the patient that permits delegates to access and search discretionary area of keen interest in a particular data. A secure index scheme that is new for keyword-search over encrypted ERMs was proposed by Yu-Chi, Kuo-Chang, Yi-Jheng, & Gwoboa (2013); this was referred to as P-index. Smaller false positive on flexible storage space and a secured, well protected channel are the main ingredients of P-index. A hybrid security solution that has to do with simple object access protocol/extensible markup language (SOAP/XML) in conjunction with secure hash algorithm version1 and advanced encryption standard and was proposed by Kiah, Abdulnabi, Zaidan & Zaidan (2013). Alanazi, Zaidan, Mat Kiah, Zaidan, and Al-Bakri (2014) built a hybrid system using AES and NTRU to improve EMR security. However, AES cannot achieve the requirement of non-repudiation alone. Thus, non-repudiation and simultaneously attainment of confidentiality during EMR transmission is made possible by the NTRU cryptography algorithm used. Ciphertext-policy attribute-based encryption (CP-ABE) has a new model with partially hidden access structure was proposed by Lixian, Junzuo, Robert, and Yingjiu (2016). Access control of encrypted data in the cloud that are fine-grained is made possible by CP-ABE. A cost-efficient and exceptional secure channel free searchable encryption (SCF-PEKS) scheme for EMRs that are sharable was proposed by Yilun, Xicheng, Jinshu, & Peixin (2016). This scheme achieves better computation performance, reduces the storage overhead, and guard against keyword guessing attacks. The Advanced Encryption Standard (AES) operation that does not derail and hinder the speed of data transmission was applied by Mikhael, Kuspriyantoa, Noor, & Edi (2017). A novel Secure Channel Free Public key encryption without designated server (SCF-wdPEKS) scheme, with the distinction of no designated server and contributes to the opposition of the existing known three types of keyword guessing attacks, was proposed by Yang & Jiguo (2018). A blockchain-based information management system, MedBlock, to handle patients' information was proposed by Kai, Shangyang, Yanhui, Hui, & Yintang (2018). The distributed ledger of MedBlock allows the efficient EMRs retrieval and access. Information security that is high combining the symmetric cryptography and custom-made access control protocols is exhibited by MedBlock. A multiparty computation protocols that is secured which gives entry for a group of distrustful data owners to cooperate jointly in executing queries that are analytical in nature against their data while exposing absolutely nothing about the entire dataset was proposed by Ahmed, Sahar, & Tarek (2018). Privacy-preserving query processing on horizontally partitioned medical data stored electronically within a group of hospitals that have no interest whatsoever in distributing their confidential data was made possible by a technique. However, cooperation is needed by all for queries to be answered about the medical history of a patient.

4.0 Discussions of Findings

Considering the outcome of the literature review, various EMR security architectures were proposed with aim to provide secure utilization of EMRs. These architectures are categorized into three groups: Hybrid, Novel, Cryptography and emerging paradigms respectively, as shown in Table 1. The

categorization is based on the architectural components: hybrid comprises of the combination of various security services; novel comprises of new innovative techniques; cryptography comprises of symmetric and asymmetric encryption services; and emerging paradigms comprise of computing technologies such as blockchain and smart contract services.

Table 1 : Categorization of Proposed Architectures

S/N	Category of Proposed Architecture	Literature Reviewed
1	Hybrid	(Mat Kiah, Mohamed, Zaidan, & Zaidan, 2013) (Alanazi, Zaidan, Zaidan, Mat Kiah, & Al-Bakri, 2014)
2	Novel	(Yu-Chi, Kuo-Chang, Yi-Jheng, & Gwoboa, 2013) (Ahmed, Sahar, & Tarek, 2018)
3	Cryptography	(Josh, Melissa, Eric, & Kristin, 2009) (Lixian, Junzuo, Robert, & Yingjiu, 2016) (Yilun, Xicheng, Jinshu, & Peixin, 2016) (Mikhael, Kuspriyantoa, Noor, & Edi, 2017) (Yang & Jiguo, 2018)
4	Emerging Paradigms	(Kai, Shangyang, Yanhui, Hui, & Yintang, 2018)

These proposed architectures, though effective in reaching their specific objectives; collectively suffers from confidentiality of the medical records, compromise of the pseudorandom permutation function, scalability, and heavy computation cost. Therefore, there is a need to improve on existing security techniques to mitigate the aforementioned issues.

Furthermore, the use and adoption of EMR poses a concern. To highlight these concerns, a broad category based on People Barrier (PB) and Technological Barrier (TB) were considered. People Barriers are the challenges that arise as a result of human influence, such as the health care provider, patients or other users of the EMR. While the Technological Barriers arise from the execution and use of the technologies that support the successful implementation of the EMR. Table 2 shows the various barricades the use and adoption of EMRs experiences.

Table 2: Category of Barricades the use and adoption of EMR experiences

S/N	Use and Adoption Barriers	People Barrier	Technological Barrier
1	Time	Yes	No
2	Lack of Technical Ability	Yes	No
3	Password distribution	Yes	No
4	Typographic Errors	Yes	No
5	Cost of implementing EMR	Yes	Yes
6	Fear about Security and Privacy	Yes	No
7	Doctor-patient interaction	No	Yes
8	Navigation Intricacy	No	Yes
9	Lack of technical Support	Yes	Yes
10	Interoperabilit	No	Yes

	y		
11	Concerns about Data Entry	Yes	Yes
12	Inadequate Data Exchange	No	Yes
13	Integration with other Health Institutions	No	Yes
14	Timely-Availability of Data	No	Yes

5.0 Conclusion

EMR have been able to solve many of the problems associated with the manual method of patient records and has been in use since 1972. Despite the solutions EMR presents to medical professionals, their adoption has not been encouraging and patients are still faced with the problems associated with manual record system. The low acceptance of EMR from literature has been attributed to security concerns related to EMRs. This study presented a review of EMR, security concerns and security frameworks proposed to improve the security concerns of EMRs. This research was able to provide an insight into the security concerns of EMRs, as well as, the barriers in use and adoption of EMR by health institutions which will bring about improved health services, especially in developing countries were manual record system are still prominent.

5.1 Recommendation

This study is recommended to hospitals, clinics, medical practitioners and other healthcare institutions that wants to improve their medical record system and also enhance the security and privacy of their client's confidential health data. It recommended that further studies be conducted on EMRs in other to address other challenges such as lack of technical Support, interoperability, error in data entry, unavailability of infrastructures in developing countries, which has also influenced against its slow adoption

II. REFERENCES

[1]. Abdul-Rahim, F., Salahuddin, L., Ismail, Z., & Samy, N. (2016, November). Safety and Privacy Issues of Electronic Medical Records. Indian Journal of Science and Technology, 9(42), 1-8. doi:10.17485/ijst/2016/v9i42/100811

[2]. Ahmed, T., Sahar, S., & Tarek, S. (2018, March 12). Privacy-Preserving Secure Multiparty Computation on Electronic Medical Records for Star Exchange Topology. Arabian Journal for Science and Engineering, 1-10. doi:https://doi.org/10.1007/s13369-018-3122-5

[3]. Ajami, S., & BagheriTadi, T. (2013). Barriers for Adopting Electronic Health Records (EHRs) by Physicians. Acta Informatica Medica, 21(2), 129. doi: 10.5455/aim.2013.21.129-134

[4]. Alanazi, O., Zaidan, A., Zaidan, B., Mat Kiah, L., & Al-Bakri, H. (2014). Meeting the Security Requirements of ElectronicMedical Records in the ERA of High-Speed Computing. Journal of Medical Systems, 165-178. doi:10.1007/s10916-014-0165-3

[5]. Cowie M. R., Blosmster J. I., Curtis L. H., Duclaux S., Ford I., Fritz F., Goldman S., Janmohamed S., Kreuzer J., Leenay M., Michel A., Ong S., Pell J. P., Southworth M. R., Stough W. G., Thones M., Zannad F., Zalewski A. (2016). Electronic health records to faciltate clinical research. Clinical Research in Cardiology, 2017; 106(1): 1 - 9. Pulished online 2016 Aug 24. doi:10.1007/s00392-016-1025-6.

[6]. Josh, B., Melissa, C., Eric, H., & Kristin, L. (2009). Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records. Microsoft Research, 103-114.

[7]. Kai, F., Shangyang, W., Yanhui, R., Hui, L., & Yintang, Y. (2018, June 12). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. Journal of Medical Systems, 1-11. doi:https://doi.org/10.1007/s10916-018-0993-7

[8]. Kiah, M., Abdulnabi, S., Zaidan, B., & Zaidan, A. (2013, September 14). An Enhanced Security Solution for Electronic Medical Records Based on AES Hybrid Technique with SOAP/XML and SHA-1. Journal of Medical Systems, 1-18. doi:10.1007/s10916-013-9971-2

[9]. Lixian, L., Junzuo, L., Robert, H. D., & Yingjiu, L. (2016). Ciphertext-policy attribute-based encryption with partially hidden access structure and its application to privacy-preserving electronic medical record system in cloud environment. SECURITY AND COMMUNICATION NETWORKS, 1-17. doi:10.1002/sec.1663

[10]. Liu, W., & Park, E. K. (2012). e-Healthcare security solution framework. 2012 21st International Conference on Computer Communications and Networks, ICCCN 2012 - Proceedings. https://doi.org/10.1109/ICCCN.2012.6289239

[11]. Lynn, W., Joy, M., & Rogers, S. (2017, December 22). Impact of Electronic Medical Records on Healthcare Delivery in Kisii Teaching and Referral Hospital. Medical & Clinical Reviews, 3(4:21), 1-7. doi:10.21767/2471-299X.1000062

[12]. McDermott, D., Kamerer, J., & Birk, A. (2019). Electronic Health Records. International Journal Of Cyber Research And Education, 1(2), 42-49. doi: 10.4018/ijcre.2019070104

[13]. Mikhael, B. R., Kuspriyantoa, Noor, C. B., & Edi, R. (2017). Securing electronic medical record in Near Field Communication using Advanced Encryption Standard (AES). Technology and Health Care, 1-6. doi:10.3233/THC-171140

[14]. NasserH.Zaied, A., Elmogy, M., & Abd Elkader, S. (2015). Electronic Health Records: Applications, Techniques and Challenges. International Journal Of Computer Applications, 119(14), 38-49. doi: 10.5120/21139-4153

[15]. Noraziani, K., Nurul' Ain, A., Azhim, Z., Sara, E., Bilal, D., Sharifa, W., & Siti, A. (2013, October 1). An Overview of Electronic Medical Record Implementation in Healthcare System: Lesson to Learn. World Applied Sciences Journal, 25(2), 323-332. doi:10.5829/idosi.wasj.2013.25.02.2537

[16]. Nzioka, C., Osumba, M., Cheburet, S., Barsigo, A., Kimanga, D., Vakil, S. and Siganga, W. (2010). Standards and guidelines for electronic medical record system in Kenya. Institutional Training & Education Centre for Health, 1–112. Retrieved from https://www.ghdonline.org/uploads/Standards_and_Guidelines_for_Electronic_Medical_Record_Systems.pdf

[17]. Pamela, A., & Sandra, A. (2014). Privacy Issues with the Electronic Medical Record. Annals of Nursing and Practice, 1(2), 1-5.

[18]. Plachkinova, M., Alluhaidan, A., & Chatterjee, S. (2015). Health records on the cloud : A security framework. International Conference on Health Informatics and Medical Systems, 15(2), 152–158.

[19]. Randy, W. (2008). Digital Polyclinic: A Distributed Electronic Medical Record System for the Underprivileged. Retrieved from The Digital StudyHall: dsh.jeejio.com/DPC_DB08

[20]. Senese, S. (2015). A study of access control for electronic health records. Governors State University. Retrieved from https://opus.govst.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1056&context=theses

[21]. Yang, L., & Jiguo, L. (2018). Efficient searchable public key encryption against

keyword guessing attacks for cloud-based EMR systems. Cluster Computing, 1-15. doi:https://doi.org/10.1007/s10586-018-2855-y

[22]. Yilun, W., Xicheng, L., Jinshu, S., & Peixin, C. (2016). An Efficient Searchable Encryption Against Keyword Guessing Attacks for Sharable Electronic Medical Records in Cloud-based System. Journal of Medical Systems, 1-9. doi:10.1007/s10916-016-0609-z

[23]. Yu-Chi, C., Gwoboa, H., Yi-Jheng, L., & Kuo-Chang, C. (2013, October 26). Privacy Preserving Index for Encrypted Electronic Medical Records. Journal of Medical System, 1-7. doi:10.1007/s10916-013-9992-x

Cite this article as :

Nkem D. Obaloje, Monday O. Eze, "Electronic Medical Record and Security Concerns", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 4, pp. 235-246, July-August 2020. Available at doi : https://doi.org/10.32628/CSEIT206441
Journal URL : http://ijsrcseit.com/CSEIT206441