How to Cite:
Ang, D., & Edo, O. C. (2022). Healthcare information system: A public healthcare facility framework. *International Journal of Health Sciences*, *6*(S2), 15140–15147. https://doi.org/10.53730/ijhs.v6nS2.9002

Healthcare information system: A public healthcare facility framework

David Ang
Auburn University Montgomery, Dept. of IS, College of Business
Corresponding author email: dang@aum.edu

Onome Christopher Edo
Auburn University Montgomery, Dept. of IS, College of Business
Email: oedo@aum.edu

***Abstract*---**The 21st century has seen innovations in information technology and the healthcare sector is not left behind. Patient healthcare record has witnessed a transformation from a paper-based model to an electronic health-based system, more importantly, cloud-based frameworks have been suggested for storing and managing patient health record. However, security and privacy concerns have been an impediment and the relationship between suggested design and adoption is unclear. In this paper, we propose a framework from a public healthcare perspective that expressly captures patient records and stores these records in a secure database and is accessible for retrieval by authorized medical personnel and researchers. The framework aims to capture patient information with a unique security identifier and provides access within the infrastructure flow to the medical personnel on demand for effective diagnosis.

***Keywords*---**electronic health-based system, healthcare database, cloud-based.

Introduction

Advances in technology have revolutionized the dynamics of storing and managing patient data. From antecedents, patient health records emanated from papyrus, with doctors and medical officers hand-charting and transcribing patient records [1] This was an arduous task, and most worrisome was the effectiveness and efficiency of managing disparate healthcare records, especially when the patient had visited several healthcare facilities. Consequently, managing health records across diverse healthcare facilities became cumbersome, and a necessity. Patient records include but are not limited to diagnosis, lab test

results, medications, patient visits, in-patient admittance reports, results, medical history, treatment, biographic data, and predictive treatment recommendations, which required a secured privacy infrastructure, this was lagging before the 21st century.

However, with recent technological innovations, Electronic Healthcare Record Systems have now emerged, with the use of database platforms and infrastructure for managing patient records in the digital space. Further advancement has evolved, conceptualized as cloud computing, which is currently chanting the lead in storing massive data. Cloud computing facilitates the storage and management of data of more than one exabyte, approximately one billion gigabytes, with infrastructure and applications to access these data remotely via the web and other software applications. Thus, enabling seamless data sharing across healthcare, facilitating interoperability and swift healthcare service delivery.

While it has been appraised for its storage capacity, cost savings, and efficiency, it has become attention for debate on one hand, and a sought-after infrastructure in the digital and medical sphere on another hand. Although the efficiency and accessibility could be attested to by users, there are however downsides with the operations of cloud-based infrastructure especially concerning privacy and security of sensitive data, with patient records falling within this domain. Furthermore, the proliferation of fragmented databases operating with the private and public clouds increases the propensity to spy, modify and steal patient medical data.

Patient medical data are often spread or fragmented across several cloud databases, and this negates the dynamics of interoperability and data sharing which is hoped to foster effective healthcare management records. The security and privacy concern still exists because of the standard of governance concerning medical record cloud administration. Cloud-based infrastructure is controlled by the owner and as such susceptible to trust and untoward activities [2] Unauthorized medical personnel are also another concern in this realm, as they could have access to sensitive data which they are not qualified to access and may not be psychologically equipped with the ethics of confidentiality to keep such data.

There are several pertinent issues that have not been wholly considered by prior studies, such as security, operability, ease of access, and data capturing and accuracy. The intent of this paper is to address these pertinent issues in the healthcare management information systems domain. The next section will be a review of literature, followed by a discussion of our proposed framework in section three, the proposed framework will be explained in section four and section five will conclude the paper.

Literature Review

The design and implementation of a universal electronic healthcare information system have been on the front burner for researchers and medical entities and has since gained worldwide attention with mixed findings and recommendations;

security lapses and privacy concerns have been topmost on the implementation factors. Although the United States has a more robust approach to safeguarding health data. However, there still exists a breach, with over twenty-five million healthcare data breach in 2017 through 2019 [3]

[4] proposed a model for the implementation of medical data security in a cloud system, they proposed a data encryption framework for encrypting patient data before upload to the cloud storage infrastructure, the model follows a sequence of seven-step activity that allows upload of the medical record and gives authorized personnel access to retrieve the patient medical record. while the idea is applauded for its uniqueness and perceived data security, it, however, follows a sequence that may be time-consuming especially with attending to patients in an emergency.

[5] proposed a hybrid technique with an inference control methodology that drives data confidentiality from indirect access, the model adopted the use of query set size restriction and k-anonymity to ensure individuals' privacy, with this model the users can access the web interface through their credentials and access the patient data through an approved query form which is directed through a middle server. While this proposed model aims to enhance security and privacy, it does not take account of patient data capturing stages and other physical security technology architecture.

[6] proposed the design and implementation of an electronic healthcare system within the cloud framework, using a modified modelling language, with hardware design and user specific access, which consist of the user, the workstation, and the server, using MYSQL to design the database and Apache webserver to host the application, with this system, authorized users have direct access to patient data and perform role-based activities within the hospital setting.

[7] proposed a secure and dependable e-health model, after a succinct review of 110 high impact research in cloud-based healthcare record management domain. Their model is based on a dual access control technique, with the patient gaining sole control of the system, and appointing or granting a medical officer access to his records which is stored in the cloud through an Access Control List security model and the activities regulated through a Mandatory Access Control security model in alignment with the registered medical facility selected by the patient. Similarly [8] studied the investigation of biometrics in the healthcare environment, the study was focused on identifying patients in the healthcare environment and they proposed an integration of periocular biometrics with a patient index in the healthcare information system, the model only seeks to enhance retrieval and identification of patient data in real-time, upon arrival to the healthcare.

In another study [9] underscore the need for managing and securing vast patient data and proposed a cloud-based model for enhancing privacy and confidentiality through the use of biometric authentication, their model is based on a behavioral signature authentication with the use of two components, the health data store, for data retrieval and the health security manager for authentication via signature biometrics, authorized users can access patient data through the use of biometric

signatures captured on the tablet and authenticated through the dynamic features of the user signature. While the methodology offers an enhance privacy approach towards accessing patient data in a cloud repository, it is pertinent to mention that access control does not guarantee data privacy or security, more so , there have been concerns about the use of behavioral signatures. [10] examined diverse behavioral signature techniques and concludes that signatures may change over time and a person's signature sketch may differ in the long run due to some uncontrollable factors and as such, impairing the authentication of the user.

Results from literature on healthcare databases using a cloud architecture have been diverse and has made relevant contributions on different scale. However, most studies have shed light on security concerns and privacy, others have proposed a technology model for securing healthcare data. While focusing on these pertinent issues, studies have proposed the design of these technology on a wider scale, and until now and to the best of our findings, there is no confirmatory evidence of the implementation of those proposal. It is our opinion that the proposals are too sizeable and lacks test capability for data security and integrity More so, in a technical study such as this, we are of the opinion that proposed models should be tested at a micro level, to test for impediments and improve the process flow across board when implemented. On another note, trust and reputation are important parameters in a cloud environment [11] Thus, given the predominance of these factors, our study addresses these issues and extend previous studies, in the rest of this paper, we provide a thematic review of our proposed model and discuss the process flow of the model.

The Proposed Framework

A common subject of discussion within the healthcare scope has been the issue of data accuracy, privacy, and confidentiality, and it is not new to emphasize that a successful treatment relies on accurate and reliable data. While several attempts have been made to counter the prevalence of data insecurity and theft within the healthcare information system scope, we incentivize by proposing a more robust approach to the capture of patient information in healthcare facilities using a systematized model of information systems process flows that will allow for higher levels of data accuracy and integrity.

The proposed framework is an adaptation of the work of [7]. However, to close the security gaps within the architectural model and we offer a more nuanced approach towards patient record security and the ease of access to patient record with a secured authentication for medical personnel within the designated medical facility (Public health facilities). The model starts off with the data capturing phase, in figure 1 (genotype, blood group, height, weight, gender) and flows through the operation phase within the infrastructure in figure 2.

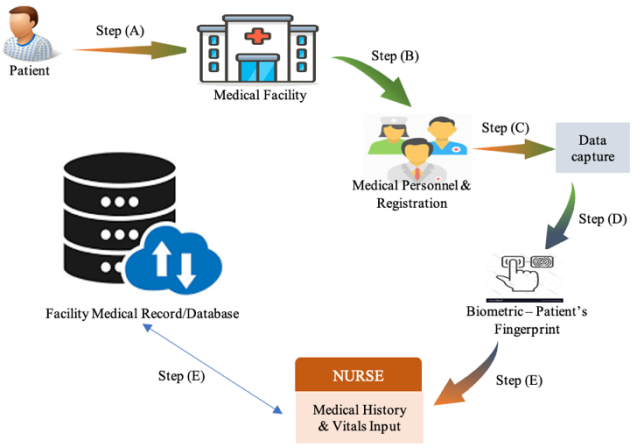

Figure 1: The Process Flow of Patient's Medical Record Data Capturing Phase

This data capturing phase is referenced on a similar architecture in the Nigerian banking system where all account holders are required to release mandatory individual identification information and cross-referenced with a valid government identification. The motive in this process is to capture patient demographic data, vital signs and biometrics which is a unique identifier to every patient. This follows a five-point step in (A) - (E) below, and as illustrated in Figure 1

A. The patient visits the nearest medical facility within his county of residence and tenders any valid identification
B. At the medical facility, the patient is received by medical record officers and is registered.
C. Upon presentation of a valid identification, the patient identification data is entered into the medical record facility.
D. To validate the patient identity and security, the patient fingerprints are taken through the biometric machine which is then cross validated with the valid identity.
E. Upon validation of the patients' biometrics and identity, the nurse requests for the patient history and take vital signs of the patient, and identifies the purpose of the patients' visit, this new information is now updated into the patient record and uploaded into the medical record facility.

Completing this stage, the data captured and stored at the medical facility would be processed and stored in the healthcare facility database which become available upon request by the onsite doctor and would give an insight into a patients' history and aid speed treatment decisions as illustrated in Figure 2 4 from steps (F) – (K).

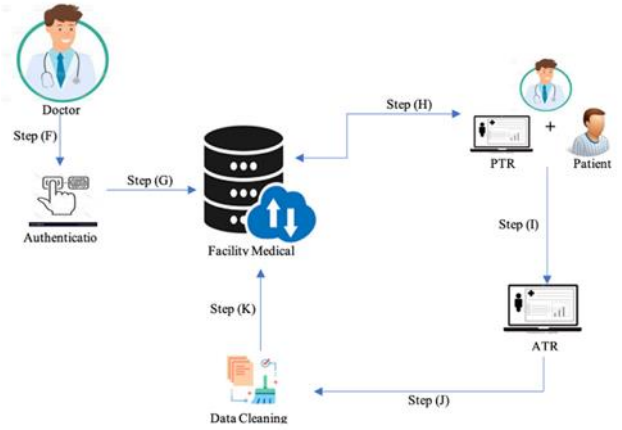

Figure 2: The Process Flow of PTR and ATR Data Capture Phase

The process flows from steps are explained below.

F. The doctor initiates and retrieves prior treatment record (PTR) from the facility database
G. Authentication is required for the doctor to access the patients' PTR, and the use of a biometric technology is one of the methods that can be deployed to verify the identity of the doctor and his access level to the information requested.
H. Upon retrieving the patient prior treatment record, the doctor is armed with the information to make accurate diagnosis and effective treatment decision, and thereafter communicates the post treatment result and observation with the patient.
I. The after-treatment record (ATR) is an update from the post treatment outcome, this new information is sent to the data cleaning facility, which is then structured and formatted for compatibility with the facility database.
J. The ATR data would be received at the cleaning facility and cleaned to fit the database structure for ease of comprehension and retrieval.
K. Facility database. The facility database is the formal and final repository where patients' records are stored for future retrieval and reference, this could be a physical data storage or a cloud-based storage.

Conclusion

Recent proposition in the information system domain has created a path towards managing patient health record, and findings have suggested a cloud-based approach for securing patient healthcare record on a global scale, with the benefit of operability and privacy. However, research is impeded by a lack of clarity on the applications and models for deployment. Thus, appearing as a utopian scheme. Consequently, it is difficult to adopt the models on miniature scale. In this paper, we emphasize on the digital aspect of effective record keeping in a healthcare information setting and introduced an easy secure access and retrieval system which is armed with a biometric technology, with this, medical personnel could have access to prior patient history, and this model could be deployed in a small setting. Thus, bridging the information system gap and the delays in patient

diagnosis.

An effective model would include one that takes cognizance of security concerns, interoperability within interacting medical facilities, effective security architecture, ease of use and a moderating entity such as the public healthcare administrator in the state or country. Once we have applied this model, and its operations in a practical environment, we would gain new insights towards advancing the model and integrating healthcare information record at a county and state level with an e-governance approach. Our future research will be exploring the integration healthcare information record at various county public healthcare facilities within a state e-governance framework.

References

1. R. F. Gillum, “From papyrus to the electronic tablet: A brief history of the clinical medical record with lessons for the digital age,” *American Journal of Medicine*, vol. 126, no. 10. 2013, doi: 10.1016/j.amjmed.2013.03.024.
2. X. Zhang, X. Yang, J. Lin, G. Xu, and W. Yu, “On Data Integrity Attacks Against Real-Time Pricing in Energy-Based Cyber-Physical Systems,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 1, 2017, doi: 10.1109/TPDS.2016.2546259.
3. S. Adler, “Largest Healthcare Data Breaches of 2021,” 2021. [Online]. Available: https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/.
4. M. Gorata, A. M. Zungeru, M. Mangwala, and J. Chuma, “Design and implementation of security in healthcare cloud computing,” *J. Comput. Sci.*, vol. 13, no. 2, pp. 34–47, 2017, doi: 10.3844/jcssp.2017.34.47.
5. M. K. Kundalwal, K. Chatterjee, and A. Singh, “An improved privacy preservation technique in health-cloud,” *ICT Express*, vol. 5, no. 3, 2019, doi: 10.1016/j.icte.2018.10.002.
6. V. Samuel, A. Adewumi, B. Dada, N. Omoregbe, S. Misra, and M. Odusami, “Design and Development of a Cloud-Based Electronic Medical Records (EMR) System,” in *Data, Engineering and Applications*, 2019.
7. N. A. Azeez and C. Van der Vyver, “Security and privacy issues in e-health cloud-based system: A comprehensive content analysis,” *Egyptian Informatics Journal*, vol. 20, no. 2. 2019, doi: 10.1016/j.eij.2018.12.001.
8. J. Mason, R. Dave, P. Chatterjee, I. Graham-Allen, A. Esterline, and K. Roy, “An Investigation of Biometric Authentication in the Healthcare Environment,” *Array*, vol. 8, 2020, doi: 10.1016/j.array.2020.100042.
9. K. A. Shakil, F. J. Zareen, M. Alam, and S. Jabin, “BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 32, no. 1, 2020, doi: 10.1016/j.jksuci.2017.07.001.
10. I. Majeed Alsaadi, “Study On Most Popular Behavioral Biometrics, Advantages, Disadvantages And Recent Applications : A Review,” *Int. J. Sci. Technol. Res.*, vol. 10, p. 1, 2021, [Online]. Available: www.ijstr.org.
11. M. Chiregi and N. J. Navimipour, “Trusted services identification in the cloud environment using the topological metrics,” *Karbala Int. J. Mod. Sci.*, vol. 2, no. 3, 2016, doi: 10.1016/j.kijoms.2016.06.002.

12. Widana, I.K., Sumetri, N.W., Sutapa, I.K., Suryasa, W. (2021). Anthropometric measures for better cardiovascular and musculoskeletal health. *Computer Applications in Engineering Education*, *29*(3), 550–561. https://doi.org/10.1002/cae.22202