International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Challenges of Information Security and Assurance on Electronic Medical Record Systems: A Review of Implementation and Applications in Tanzania

Daudi Mashauri[1], Pankras Kandengukila[2]

[1]Assistant Lecturer, Tanzania Institute of Accountancy (TIA), Dar es Salaam, 15108 Tanzania.
[2]Assistant Lecturer, Tanzania Institute of Accountancy (TIA), Singida, Tanzania.

Abstract
Over the last decade, methods for collecting, storing, organizing, analyzing, and communicating information have been vastly influenced by the application of Information Communication Technology (ICT) tools. Demands for electronic health (eHealth) systems in Tanzania are enormous. This demand resulted from the inconveniences of paperwork-based information processing. With the primary focus on implementing and applying eHealth systems, aspects of security and privacy of electronic medical records (EMR) often need to be considered. However, medical records are sensitive and require a high degree of confidentiality and integrity. This paper articulates information security and assurance challenges in EMR system implementation and application in Tanzania. The paper adopted a peer review of published articles. An analysis of the current state of application of the eHealth system in Tanzania was conducted. Diverse EMR systems are being used in Tanzania hospitals. Information security should be prioritized during the implementation and application of these EMRs. Furthermore, data integration among systems still needs to be implemented. Several factors constrain the performance of secured EMR: inadequate budget allocation, lack of technical support, security threats and vulnerabilities, and user resistance. Finally, a recommendation for a secure EMR system and further research on improved security and reliable eHealth system is outlined.

Keywords: Electronic medical record; information system; information security and assurance; Tanzania.

1. Introduction

Advancements in ICT for the last decade have created a spillover effect across all social, economic, and political sectors. In almost every industry, information systems have been adapted to eliminate shortfalls from manual paper-based systems. Information systems can collect, organize, store, process, and share information for decision-making. In the medical industry, electronic health systems are used with various modern digital tools such as mobile devices, online or e-learning tools, decision support systems, telemedicine, health information systems (HIS), and EMRs [1]. An electronic health record can be defined as a digital version of a patient's paper chart [2].

In 2015, the United Republic of Tanzania's government launched an ambitious plan to create the Government of Tanzania Hospital Management Information System (GoT-HoMIS) [3]. The system aims to collect and report facility-level clinical information while supporting public health facilities in service delivery and management. Furthermore, the medical industry in Tanzania conflates public and private facilities. Some facilities use open-source EMR systems, while others use closed sources owned by third-party companies [4]. Medical records are sensitive and require a high degree of trust during handling. Integrity and confidentiality issues must be addressed when implementing EMR projects in Tanzania. However, security and privacy issues must be addressed appropriately as they influence the acceptance and use of EMR systems [5]. The implementation and application of EMR systems can be assessed by considering aspects of information security and assurance.

The National Institute of Standards and Technology (NIST) defines information security as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability" [6]. Implementing confidentiality means focusing on protecting personal and proprietary information from unauthorized access and disclosure. Integrity protects both data and the system against improper modifications or destruction. Availability ensures uninterruptable and timely access to the system and information. Information assurance is the degree of confidence in security mechanisms to protect and defend both systems and information [6]. The notion of information assurance is encircled to ensure five objectives: authentication, availability, confidentiality, integrity, and non-repudiation. Authentication is the process of validating the identity of system users through what a user knows, like a password; what a user has, like a token or ID card; who a user is, like a fingerprint; and what a user can produce like voice [7]. Non-repudiation protects both senders and receivers in communication from denying their action while transmitting a message.

Information security and information assurance can sometimes be used interchangeably as they possess overlapping objectives. However, information assurance covers a broader aspect, not limited to security controls or countermeasures to protect information and information systems. In addition to proactive offensive and reactive, defensive approaches to protecting information, information assurance also comprises security professionals' accountability, coverage, and responsibilities [8]. Thus, information assurance is more holistic than information security in protecting systems and data [7]. So far, however, there has been little discussion about security concerns following implementing EMR systems in Tanzania. If the situation remains unattended, the safety of EMR systems lies at the mercy of system users. Therefore, this study reviews the current approaches, implementation, and applications of EMR systems in Tanzania and outlines challenges facing information security and assurance. Furthermore, the study presents security considerations towards a secure EMR system application in Tanzania.

Contributions of this research work can be summarized as follows:

1. Outlining EMR systems implemented at medical facilities in Tanzania;
2. Present a class of information security and assurance challenges facing EMR system applications; and
3. Providing security mechanisms to ensure EMR system confidentiality, integrity, and availability.

The remainder of this paper is presented as follows: Section 2 explains related works on EMR systems in Tanzania; Section 3 concerns the methodology used for this paper; Section 4 presents the results;

Section 5 discusses information security considerations for a secured EMR implementation; and Section 6 presents the conclusion.

2. Related works on EMR systems in Tanzania

N. Mleke & Ally Dida, (2020) conducted a qualitative survey to monitor and evaluate health projects in Tanzania. The survey collected qualitative data using document reviews, interviews, and focus group discussions. Respondents were selected using purposive sampling from the Dodoma and Dar es Salaam regions. The study found that manual paperwork and electronic database systems are used to keep health information. The study also outlined the main challenge of evaluating health projects based on manual paperwork information.

Mashoka et al., (2019) presented an electronic medical record system implementation in a resource-limited setting. The pilot project was implemented according to standard system development practice [11]. The design steps began with planning through implementation and maintenance. The project was successfully implemented at Muhimbili National Hospital in the emergency department. Basic computer skills training was provided to system users. Supercritical users were identified and assigned extra responsibility toward system usage. Though constrained by several challenges, this project successfully served the intended purpose.

Haule et al., (2019) outlined an analysis of requirements for developing a data exchange module between hospital medical systems and the National Health Insurance Fund (NHIF) claims management system. The study adapted questionnaires, interviews, and document reviews for data collection. Candidates were selected by using a random purposeful sampling technique. The study outlined several challenges resulting from the current manual claim system. The study also suggests adapting a data exchange module between hospitals and NHIF claim systems. Furthermore, the study presented a conceptual framework of a data exchange module for the proposed solution.

Mtey & Dida, (2019) presented an analysis of interoperable systems based on extensive data sharing to facilitate data sharing among electronic medical record systems. The paper adopted a document review approach. It involved peer-reviewed and grey literature on the global trend of eHealth interoperability. The work outlined several challenges to be addressed to ensure the successful implementation of interoperable eHealth systems. The challenges conflate technical and infrastructural issues.

B. R. Kikoba et al., (2019) researched to improve the collection, reporting, and use of medical data, analysis for integrating EMR, and district health information system version two (DHIS2). The study adopted a sequential exploratory approach. Five hospitals from Dar es Salaam, Pwani, and Morogoro regions were selected. A prototype was developed for EMR – DHIS2 integration. Furthermore, an analysis of the implemented prototype uncovered contributions in ensuring data availability and quality.

Kombe et al., (2019) explored security issues facing eHealth systems and presented a blockchain-based technology solution in the research work. The study adopted qualitative data collected through interviews, observation, and document analysis. Experts were selected from hospitals and health centers through purposive sampling. The study outlined issues of registration mechanisms, information sharing, data integrity, and bandwidth usage facing eHealth systems. The study proposed the adoption of blockchain technology to resolve the named challenges. Furthermore, it emphasizes that blockchain technology will improve the security and privacy of eHealth systems.

Mtebe & Nakaka, (2018) assessed EMR system implementation to evade future failures. The study was piloted at Kilimanjaro Christian Medical Center (KCMC). It adopted a qualitative method, collecting

data through interviews, focus group discussions, document reviews, and observations. The study revealed eight (8) different information systems used in various hospital functions. HarmoniMD was used as the EMR system from 2015 to the time of conducting the research. Also, the study discovered no system integration between EMR and other present information systems. Furthermore, the study suggested a user-centric system development approach for future EMRs.

Mwammenywa & Kaijage, (2018) examined whether delivering HIV/AIDS healthcare information can be enhanced through mobile applications. The study used questionnaires to collect data from HIV-positive and negative respondents and medical practitioners. It was conducted in the Dar es Salaam region. A random sampling of males and females was adopted. Questionnaires contained three main parts: demographic information, comfortability, attendance to HIV/AIDS care and treatment centres (CTC), and perception of online health information. 88.3% of respondents acknowledged the existence of HIV/AIDS CTC. Among those, 60.7% had visited at least once, and 24.5% were uncomfortable due to social stigma. 79.1% of the respondents indicated they use online media to search for health information, and 78.5% wanted access through a mobile application.

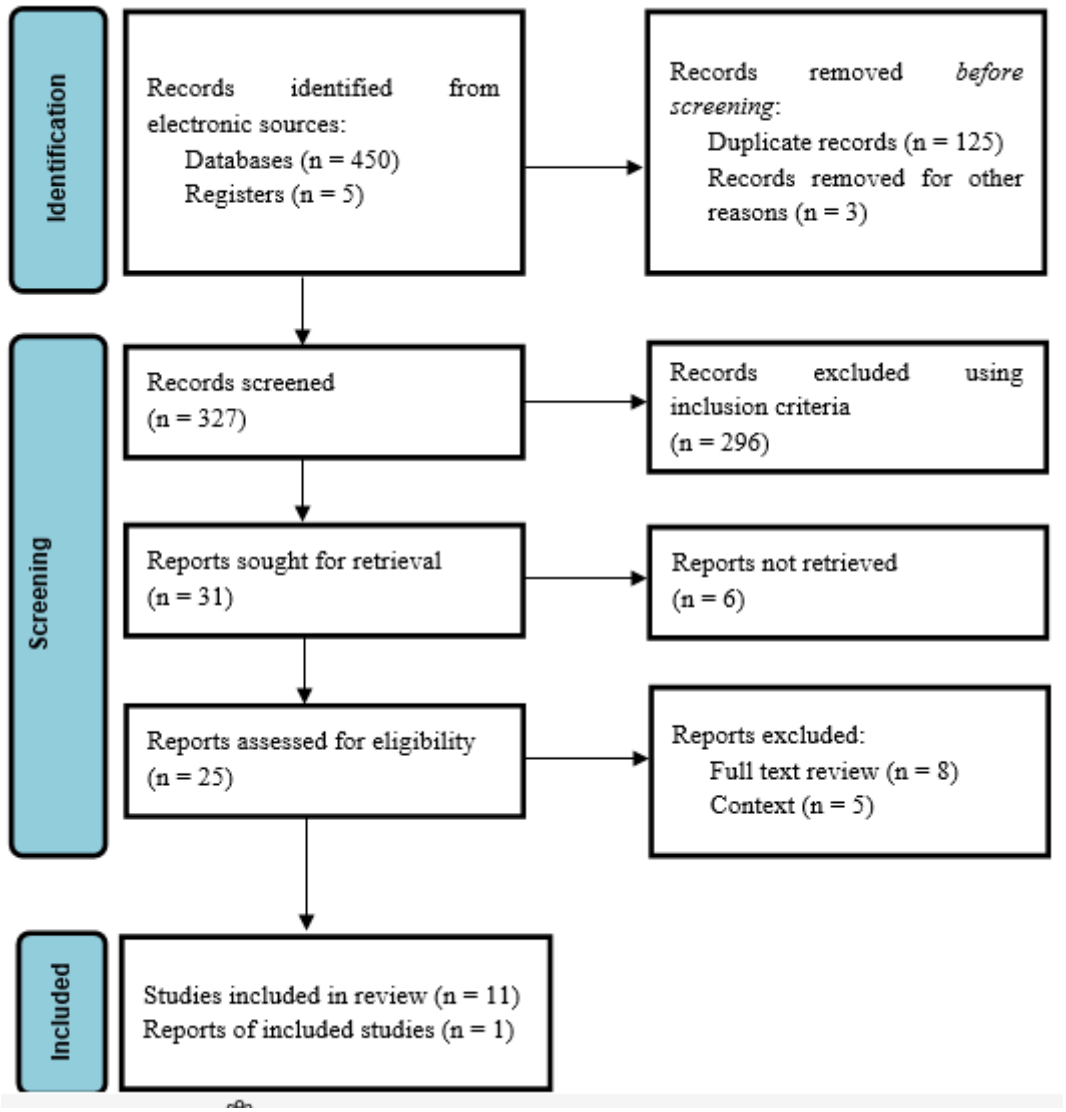
Tierney et al., (2010) researched the implementation of electronic health record systems in HIV clinics across three East African countries: Tanzania, Kenya, and Uganda. OpenMRS was developed and implemented in each of the three East African counties. Six health facilities were selected for each country as a pilot for implementing the project. In the case of Tanzania, the facilities were in Dar es Salaam, Morogoro, and Pwani regions. The study revealed that implementation was successful across all three countries. Furthermore, it showed that OpenMRS usage was influenced by three common factors: local budgetary control, academic partnership, and in-country IT support.

3. Methodology

EMR systems are a broad subject that involves the application of technological tools to facilitate the delivery of health services. The focus was on EMR systems application in the health industry as applied in Tanzania. A Boolean search on Google Scholar was conducted for indexed articles. The search queries with a combination of keywords were adopted, returning different results for each. Keywords used were: electronic medical record, health information system, hospital system, security, confidentiality, integrity, availability, and Tanzania. For example, a query "confidentiality" OR "integrity" OR "availability" of "electronic medical record systems" AND "Tanzania" returned 166 results. "Security" of "health information systems" AND "Tanzania" returned 1,100 results, whereas a query "security" of "electronic medical record systems" AND "Tanzania" returned 99 results.

The inclusion criteria were original or review articles published in English, presenting an approach, model, implementation, or application of information systems in the health sector, preferably in Tanzania or Sub-Saharan developing countries. Studies illustrating information systems in industries other than health were omitted as an exclusion criterion. Initial search results returned 455 records; articles were selected based on the topic's relevance, with the preference of papers from 2021 below the timeline. Adopting the exclusion criteria during the screening phase retained 25 articles. Then, after a full-text review of the selected articles, 13 were excluded. Selected article titles were downloaded from bibliographic databases such as Academia, ResearchGate, ScienceDirect, and PubMed. The authors conducted the whole process and adopted a PRISMA approach [18], as summarized in Figure 1.

Figure 1: Adopted PRISMA model



4. Results

It is documented that various EMR systems are being applied across medical facilities in Tanzania. Table 1 summarizes EMR systems in Tanzania with separate hospital facilities. This table is quite revealing in several ways. First, EMR systems in Tanzania conflate open-source and proprietary software. Second, several medical facilities implement multiple EMR systems simultaneously. Third, GoT-HoMIS scales and dominates in public health facilities only. Together, these results suggest the possibility of challenges resulting from islands of information systems at the facility level.

However, information security in EMR systems remains an open challenge that needs to receive the attention it deserves. Literature evidence that assesses the security strength of individual EMR systems still needs to be improved. The following subsections present the main challenges facing information security and assurance of EMR systems implementation and applications in Tanzania.

4.1 Authentication

Authentication is validating system users' identity, aiming to isolate authorized system users from unauthorized. Current EMR implementations in Tanzania use a single authentication method relying on login credentials only [3]. However, textual-based passwords are vulnerable to dictionary attacks,

shoulder surfing attacks, and accidental login [19]. This exposes EMR system users in Tanzania to the high risk of identity theft.

The choice of authentication methods is rooted in three factors: usability, security, and cost [20]. Even though using "username" and "password" can be easy to implement on EMR systems, multiple authentication methods should be adopted in EMR implementations. Furthermore, the use of biometric authentication methods like facial recognition is guaranteed to deliver both security and usability for EMR system users [21].

Table 1. A summary of EMR systems applied in Tanzania.

S/N	EMR System(s)	Medical facility
1.	AfyaPro; GoT-HoMIS	Morogoro regional hospital [14]
2.	Care2X	Mbeya referral hospital [14]
3.	Care2X; HarmoniMD	KCMC [4]
4.	DHIS2	Amana, Muhimbili, Tumbi, Morogoro and Mnazi mmoja [14]
5.	eHMS	Amana hospital [14]
6.	GoT-HoMIS	170 public health facilities [3]
7.	Jeeva	Muhimbili national hospital [14]
8.	OpenMRS	Morogoro regional hospital, Ocean Road, and Tumbi referral hospital [17]

4.2 Availability

Availability ensures uninterruptable and timely access to the EMR system and information. Poor design of EMR systems hinders information availability to health workers for informed decision-making during patient treatment [22]. Also, an Unreliable power supply remains one of the main challenges hindering Tanzania's successful implementation of EMR systems [23].

Power failure is the most critical threat to EMR system implementations. It is accompanied by server and air conditioning failure, which leads to service unavailability [24]. Also, EMR implementations in Tanzania lack technical support and inadequate digital skills among health workers [25]. Overall, this undermines the availability of EMR systems and information to users.

4.3 Confidentiality

Confidentiality protects personal and proprietary information from unauthorized access and disclosure. Current EMR system implementations in Tanzania do not guarantee confidentiality. Relying on text-based passwords, which are vulnerable [19], and inadequate digital skills among health workers [25] puts the EMR system at risk of unauthorized access and information disclosure.

However, to realize the full benefits of EMR systems, patients must be assured of the security and accuracy of their medical records [26]. To ensure the confidentiality of EMR systems, health workers must be equipped with the required digital skills and classify medical records at different levels according to their sensitivity.

4.4 Integrity

Integrity protects both data and the system against improper modifications or destruction. Due to the nature of health information system projects in Tanzania, it is common to find an EMR system deployed

along with other information systems in the same medical facility [4]. Also, various EMR systems are found to be deployed at the facility level simultaneously.

However, these systems operate as standalone, lacking system integration. Due to this problem, the organization owns islands of information systems in which data inconsistency and redundancy are unavoidable. Consequently, if the situation is unturned, data and system integrity will remain undermined.

4.5 Non-repudiation

Non-repudiation protects both senders and receivers in communication from denying their actions while transmitting a message. However, the literature in this regard still lacks EMR systems, which calls for further research. System audits must be conducted regularly on EMR applications to ensure non-repudiation. This will assist in tracking user activities and information when accessing the EMR system.

5. Discussions

The results section explains that EMR implementation projects in Tanzania conflate several security issues. With the issues remaining unattended, the security of EMR systems becomes the most intractable issue of the current digital era. However, the impact of the identified security holes can be mollified by implementing a secured EMR that can be built with information security considerations. Following subsections present the primary considerations to assure the confidentiality, integrity, and availability of patient data and the EMR system.

5.1 Confidentiality

An EMR system implementation must be secured, and patient data and related information must be kept confidential and private [27]. Confidentiality can be sought in terms of data confidentiality and secrecy. The former implies limiting data access to only authorized users. In contrast, the latter implies individuals control or influence their data about who collects and accesses them, what kind of data, and by which methods.

In the United States, approximately one-third of data breaches occur in hospitals. The theft was the leading incident, followed by unauthorized access, loss, and hacking [28]. Most EMR implementations fail to achieve security requirements without considering patients' rights to their information [29]. Cryptographic algorithms can secure data transmission in EMR systems and blockchain technologies.

To guarantee the confidentiality and secrecy of medical and related EMR systems, a Bell-LaPadula security model can be adopted in access control [30]. At the medical facility level, access to EMR system data must be classified according to the security level per organizational structure. Adapting this model will assist in limiting access to patient information and assure data confidentiality and the EMR system.

5.2 Integrity

EMR systems commonly experience integration problems when communicating with other information systems within or outside medical facilities. Medical record exchange systems can be adapted to eliminate barriers to data exchange between different EMR systems [31]. Since EMR systems are web-based, if data exchange goes unchecked, it may cause problems relating to data inconsistency. This transpires when two systems have different versions of duplicate data.

The integrity of EMR systems can be assured by adopting access control rules. Data integrity can be enhanced based on the Biba model [30]. The ability to modify data for users and programs must be classified and subjected to corresponding privileges. Furthermore, to secure EMRs in a web-based

environment, model view controlled PhP framework Laravel can be adapted to present the site from SQL injection, XSS attacks, and cross-site forgery [32]. This will provide security for web-based projects and assist in ensuring data integrity.

5.3 Availability

Availability ensures that the EMR system works and can provide users with access at the time of their need without denial. With valid login credentials, end-users must be able to access services delivered through EMR systems. Load balancing and fair access policies must be implemented in the servers to combat bottlenecking. Even though EMR systems in Tanzania are offline and standalone, mitigations against denial-of-service attacks should be implemented. Network traffic should be constantly monitored, and source addresses should be filtered to prevent spoofing. Furthermore, using host- and network-based firewalls, inbound and outbound traffic should be limited wherever possible. Also, endpoints must be patched for known vulnerabilities. Since EMR systems can also be used for stock control functions to reduce operating costs and enhance the availability of medicines and medical supplies [33], system availability must receive proper and desired attention.

6. Conclusion

This paper reviewed the current approaches, implementation, and applications of electronic medical record systems in Tanzania from an information security and assurance point of view. The aim was to identify information security and assurance challenges of EMR project implementations and applications in Tanzania and suggest security considerations towards secured EMR systems. We discovered that most EMR projects are web-based, with little or no consideration given to information security. Budget constraints also affect projects of this type, causing attention to be focused solely on system access at the expense of security. EMR systems contain sensitive patient medical records that demand integrity and confidentiality during access. In light of this, the security of the EMR system should not be an option. In this paper, we have also presented vital security considerations for a secured EMR project implementation. By observing the information security triad, which includes confidentiality, integrity, and availability, EMR systems can be secured from current security threats. Security issues must be addressed from the user's perspective to guarantee successful implementation and acceptance of the EMR system. As part of our future work, we plan to design a framework for implementing secured electronic medical record system projects. This shall be used as a guide to ensure the confidentiality, integrity, and availability of EMR projects in Tanzania and Sub-Saharan countries.

References

1. T. Gerber, V. Olazabal, K. Brown, and A. Pablos-Mendez, “An agenda for action on global e-health,” Health Aff., vol. 29, no. 2, pp. 235–238, 2010, doi: 10.1377/hlthaff.2009.0934.
2. ONC, “Frequently Asked Questions.” Accessed: Jul. 10, 2023. Online.. Available: https://www.healthit.gov/faq/what-electronic-health-record-ehr
3. President’s Office - RALG, “Government of Tanzania - Hospital Management Information System (GoT-HoMIS),” pp. 1–19, 2017.
4. J. S. Mtebe and R. Nakaka, “Assessing Electronic Medical Record System Implementation at Kilimanjaro Christian,” J. Health Inform. Dev. Ctries., vol. 12, no. 2, pp. 1–16, 2018.
5. O. Enaizan, B. Eneizan, M. Almaaitah, A. T. Al-Radaideh, and A. M. Saleh, “Effects of privacy and security on the acceptance and usage of EMR: The mediating role of trust on the basis of multiple

perspectives," Informatics Med. Unlocked, vol. 21, p. 100450, 2020, doi: 10.1016/j.imu.2020.100450.
6. M. Nieles, K. Dempsey, and V. Y. Pillitteri, "NIST Special Publication 800-12 Revision 1 - An introduction to information security," NIST Spec. Publ., 2017, Online.. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf
7. L. Cilliers, "Exploring information assurance to support electronic health record systems," 2017 IST-Africa Week Conf. IST-Africa 2017, no. January, 2017, doi: 10.23919/ISTAFRICA.2017.8102363.
8. M. Evans, L. A. Maglaras, Y. He, and H. Janicke, "Human behaviour as an aspect of cybersecurity assurance," Secur. Commun. Networks, vol. 9, no. 17, pp. 4667–4679, 2016, doi: 10.1002/sec.1657.
9. M. N. Mleke and M. Ally Dida, "A Survey of Monitoring and Evaluation Systems for Government Projects in Tanzania: A Case of Health Projects," Int. J. Inf. Eng. Electron. Bus., vol. 12, no. 1, pp. 8–18, 2020, doi: 10.5815/ijieeb.2020.01.02.
10. R. J. Mashoka et al., "Implementation of electronic medical records at an Emergency Medicine Department in Tanzania: The information technology perspective," African J. Emerg. Med., vol. 9, no. 4, pp. 165–171, 2019, doi: 10.1016/j.afjem.2019.07.002.
11. M. Kuhrmann et al., "Hybrid Software and System Development in Practice Waterfall,Scrum, and Beyond." Proceedings of International Conference on Software System Process, Paris, France, pp. 1–10, 2017. doi: 10.1145/nnnnnnn.nnnnnnn.
12. A. Haule, M. Ally Dida, and A. Elikana Sam, "Towards Data Exchange between Health Information System and Insurance Claims Management System," Int. J. Inf. Eng. Electron. Bus., vol. 11, no. 2, pp. 28–34, 2019, doi: 10.5815/ijieeb.2019.02.04.
13. M. M. Mtey and M. A. Dida, "Towards interoperable e-Health system in Tanzania: analysis and evaluation of the current security trends and big data sharing dynamics," Int. J. Adv. Technol. Eng. Explor., vol. 6, no. 59, pp. 225–240, 2019, doi: 10.19101/ijatee.2019.650057.
14. B. R. Kikoba, E. Kalinga, and J. Lungo, Integrating electronic medical records data into national health reporting system to enhance health data reporting and use at the facility level, vol. 551, no. April. Springer International Publishing, 2019. doi: 10.1007/978-3-030-18400-1_44.
15. C. Kombe, A. Sam, M. Ally, and A. Finne, "Blockchain Technology in Sub-Saharan Africa: Where does it fit in Healthcare Systems: A case of Tanzania.," J. Health Inform. Dev. Ctries., vol. 13, no. 2, p. 1, 2019, Online.. Available: http://www.jhidc.org/%0Ahttp://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=140226561&lang=pt-br&site=eds-live&scope=site
16. I. A. Mwammenywa and S. F. Kaijage, "Towards Enhancing Access of HIV/AIDS Healthcare Information in Tanzania: Is a Mobile Application Platform a Way Forward?," Int. J. Inf. Technol. Comput. Sci., vol. 10, no. 7, pp. 31–38, 2018, doi: 10.5815/ijitcs.2018.07.04.
17. W. M. Tierney et al., "Experience implementing electronic health records in three East African countries," Stud. Health Technol. Inform., vol. 160, no. PART 1, pp. 371–375, 2010, doi: 10.3233/978-1-60750-588-4-371.
18. M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," The BMJ, vol. 372. 2021. doi: 10.1136/bmj.n71.
19. S. S. Patel, A. Jaiswal, Y. Arora, and B. Sharma, "Survey on Graphical Password Authentication System," pp. 699–708, 2021, doi: 10.1007/978-981-15-8530-2_55.
20. I. Velásquez, A. Caro, and A. Rodríguez, "Authentication schemes and methods: A systematic

literature review," Inf. Softw. Technol., vol. 94, pp. 30–37, 2018, doi: 10.1016/j.infsof.2017.09.012.
21. S. Purkayastha, S. Goyal, B. Oluwalade, T. Phillips, H. Wu, and X. Zou, "Usability and Security of Different Authentication Methods for an Electronic Health Records System," 2019.
22. B. Kikoba, F. Sukums, Z. Abel, N. Shidende, Y. Kijuu, and S. Ilomo, "Assessing How Health Data Systems Support Data Use in the Tanzanian Health System 12 th Health Informatics in Africa Conference (HELINA 2019) Assessing How Health Data Systems Support Data Use in the Tanzanian," J. Heal. Informatics Africa, no. May, pp. 1–7, 2020.
23. MOHCDGEC, "Digital Health Strategy: July 2019 - June 2024," no. July, pp. 1–98, 2019.
24. G. Narayana Samy, R. Ahmad, and Z. Ismail, "Security threats categories in healthcare information systems," Health Informatics J., vol. 16, no. 3, pp. 201–209, 2010, doi: 10.1177/1460458210377468.
25. J. Peltola, "On Adoption and Use of Hospital Information Systems in Developing Countries: Experiences of Health Care Personnel and Hospital Management in Tanzania," The Nelson Mandela African Institution of Science and Technology, 2019. Online.. Available: https://trepo.tuni.fi/bitstream/handle/10024/118773/PeltolaJohanna.pdf?sequence=2&isAllowed=y
26. A. Shenoy and J. M. Appel, "Safeguarding confidentiality in electronic health records," Cambridge Q. Healthc. Ethics, vol. 26, no. 2, pp. 337–341, 2017, doi: 10.1017/S0963180116000931.
27. MHSW, "Integrated Hospital Management System Implementation," 2015.
28. M. H. Gabriel, A. Noblin, A. Rutherford, A. Walden, and K. Cortelyou-ward, "Data Breach Locations, Types, and Associated Characteristics Among US Hospitals," Am. J. Manag. Care, vol. 24, no. 2, pp. 78–84, 2018.
29. H. O. Alanazi, H. A. Jalab, G. M. Alam, and B. B. Zaidan, "Securing electronic medical records transmissions over unsecured communications : An overview for better medical governance," vol. 7, no. 11, pp. 1–16, 2020.
30. M. Cristiá and R. Gianfranco, "Automated proof of Bell–LaPadula security properties," J. Autom. Reason., vol. 65, no. 4, pp. 463–478, 2021.
31. G. Rweikiza and D. Machuve, "Reducing Fragmentation in Sharing of Information in E-Medical Recording Systems : Case of OpenMRS and Care2x Development of medical records exchange system - a case of OpenMRS and Care2X," Int. J. Adv. Technol. Eng. Explor., vol. 6, no. 52, pp. 77–83, 2019, doi: 10.13140/RG.2.2.16010.31680.
32. N. Solanki, D. Shah, and A. Shah, "A Survey on different Framework of PHP," Int. J. Latest Technol. Eng. Manag. Appl. Sci., vol. VI, no. VI, pp. 155–158, 2017, Online.. Available: www.ijltemas.in
33. S. Chiumbo, "The Influence of Jeeva Information System in Stock Control: the Case of Muhimbili National Hospital," The Nelson Mandela African Institution of Science and Technology, 2014.