Enhancing Electronic Medical Records Privacy in Tanzania: A blockchain-based framework

Happyness Hurdson* and Juliana Kamaghe
The Open University of Tanzania
**Corresponding Author 1mamsaro28@gmail.com , 2juliana.kamaghe@out.ac.tz*

DOI: *https://doi.org/10.61538/huria.v33i1.1965*

Abstract

Electronic Medical Records (EMRs) are vital for healthcare delivery in Tanzania, yet centralised systems in government hospitals remain vulnerable to privacy breaches, unauthorised access, weak access controls, and insufficient audit trails. This study proposes a blockchain-based framework to strengthen EMR privacy in Tanzanian public hospitals, overcoming limitations of existing firewall-based protections. Using a mixed-methods design, data were collected at Dodoma Regional Referral Hospital from 210 purposively sampled participants (108 staff, 102 outpatients) via questionnaires, structured interviews, and expert interview was used during framework validation. Quantitative analyses using SPSS and EPI Info, and thematic qualitative analyses, revealed key privacy gaps: 75.9 percent of staff used unencrypted, password-protected files for data transfer; 72.2 percent reported unclear access roles and policies; and 64.7 percent of patients expressed serious concerns about EMR confidentiality due to limited awareness of data-handling practices. The proposed permissioned blockchain framework integrates Proxy Re-Encryption (PRE) to enable secure, consent-based sharing, immutable smart-contract audit trails, and off-chain encrypted storage. This enables controlled access by hospital staff and authorised third parties (e.g., insurance providers) while preserving patient privacy. Expert validation through scenario-based review and prototype testing confirmed technical feasibility, alignment with Tanzania's Personal Data Protection Act, and effectiveness in addressing vulnerabilities, including password sharing and a lack of traceability. This tailored solution offers a scalable approach to privacy-preserving EMR management in resource-limited settings, with potential for broader adoption across Sub-Saharan Africa.

Keywords: *Privacy, Electronic medical records, Medical Records, Proxy Re-Encryption, Blockchain technology*

INTRODUCTION

Electronic Medical Records (EMR) have become a powerful tool in modern healthcare delivery. EMRs significantly improved the safety and quality of healthcare delivery by increasing access to health information, reducing illegibility, and enabling closer oversight of clinical care processes. In the healthcare sector, the first attempts to create digital versions of electronic medical records (EMRs) were made in 1962 within the Oxford Record Linkage Project (ORLP) (Acheson & Evans, 1964). The current EMR system has significant flaws that compromise patients' privacy and safety and reduce medical practitioners' trust in EMR data (Haux, 2006). Patients cannot control who can access their confidential information. There is also no mechanism to assess the privacy, Security, and trustworthiness of patients' medical data (Choi, Capian, Krause, & Streeper, 2006).

The implementation of EMR system faces several challenges. More government support and adequate infrastructure are needed, including reliable internet connectivity and limited computer access, which hinder successful deployment (Munyaradzi C, Katurura, Cilliers L, 2018). Healthcare professionals' resistance and patients' lack of awareness of the benefits of EMRs pose significant obstacles (Daria, Kok N, Basoglu, Daim T, 2019). Patient participation and education are crucial for effective utilisation of EMRs. Cost is another barrier, especially in resource constrained settings, with initial expenses, ongoing maintenance fees, and training costs.

Blockchain technology offers a promising solution for achieving data-sharing privacy preservation, thanks to its immutability (meaning the data or ledger is permanent and tamper-proof, and its history cannot be modified after its creation). Hence, a distributed, searchable scheme for electronic medical records is proposed by implementing blockchain technology. Blockchain-based access control technology provides a range of strategies to address privacy concerns and ensure the confidentiality of patient information.

Blockchain technology strategies encompass robust encryption, access controls, user authentication mechanisms, and privacy assessments. Blockchain is a public, decentralised, append-only, immutable digital ledger with a time-stamped series of transactions called blocks that are linked to form a chain, secured by cryptographic principles such as public-key cryptography. This study aims to develop and test a blockchain framework to enhance EMR privacy in Tanzanian government hospitals.

The purpose is to provide secure data transactions, reduce compliance costs, and expedite data transfer processing.

Tanzania's healthcare sector faces critical challenges in Electronic Medical Record (EMR) privacy and Security, with only 34.5 percent of healthcare facilities achieving full EMR implementation, while 78 percent rely on basic DHIS2 systems (Chakravarthy et al., 2025). Current centralised EMR architectures create significant vulnerabilities that threaten patient privacy and data integrity in resource-constrained environments.

The core problems include centralised systems that create single points of failure, making patient data vulnerable to unauthorised access and malicious attacks (Mwamba & Mjema, 2024). Healthcare facilities report difficulties in safely sharing medical information between institutions, maintaining data integrity, and implementing adequate access controls (Charles, 2024). Weak audit mechanisms prevent the tracking of unauthorised access, undermining patient trust and violating medical confidentiality principles. Additional challenges include bandwidth constraints, off-chain cloud storage vulnerabilities, and inadequate regulatory frameworks for health data protection (Hao et al., 2025).

Institutional gaps compound these technical vulnerabilities. Health administrators and policymakers demonstrate limited awareness of advanced security solutions, while human capacity deficits hinder the deployment of sophisticated privacy-preserving technologies (Hao et al., 2025; Tandon, 2022). Infrastructure limitations, including unreliable connectivity and scalability concerns for storage, further complicate EMR security enhancement efforts. Blockchain technology offers promising solutions through decentralised architectures, cryptographic integrity protection, and intelligent contract-based access control (Chakravarthy et al., 2025; Hao et al., 2025; Kumbo et al., 2024). Prototype systems have demonstrated feasibility, with implementations successfully tested on 200,000 EMRs using privacy-preserving techniques. However, critical gaps remain: limited real-world deployment in developing countries, insufficient adaptation to resource-constrained environments, limited interoperability with existing systems, and inadequate training frameworks. A tailored blockchain-based framework addressing Tanzania's specific technical, institutional, and resource constraints is essential for protecting patient privacy while enabling digital healthcare transformation across Sub-Saharan Africa. Moreover, healthcare records were stored in centralised databases, making healthcare data a highly attractive target for attackers. Several research studies have shown that centralisation increases

privacy risks and requires trust in a single authority. Centralised databases can leave us vulnerable to attacks that escalate into cyber threats, ranging from the recent ransomware attack (Mohurle & Patil, 2017) to the Equifax attack, which compromised the privacy of electronic medical records (Berghel, 2017). The objectives are to assess the current privacy controls in government hospitals, identify specific points at which unauthorised access or disclosure occurs, and test a blockchain-based framework that enables controlled sharing and strong privacy protection. The proposed framework seeks to offer secure transactions, reduce privacy risks, and support safe information exchange in public hospitals

LITERATURE REVIEW

Privacy factors play a significant role in the acceptance of healthcare technology (Wilkowska & Ziefle, 2011). Although EMRs offer many advantages, current technologies are insufficiently utilised to realise their full potential while maintaining patients' privacy. Healthcare adopters and doctors remain deeply concerned about the privacy and Security of patients' data, which remains inadequately addressed. Moreover, privacy and security concerns remain significant barriers to EMR adoption (Ochieng & Hosoi, 2005). (AL-nassar, Abdullah, & Osman, 2009) believes that understanding these barriers and developing an appropriate strategy to address them will ensure the success of EMR implementation. The most common problems encountered by EMR users are Security, privacy, and confidentiality (George & Bhila, 2019). There are many challenges in EMR implementation, including legal issues such as privacy and security, as well as insufficient standards for EMR users. This is why is considered a critical issue for doctors and patients.

The research was done by (Wang, 2015) from Taiwan about the Security and privacy of personal health records, electronic medical records and health information. The analysis was based on 13,960 citations of 410 articles, and the results indicate that the designer of the electronic health information system must avoid unauthorised use and cyberattacks. Wrongful disclosure of individually identifiable health information was an offence punishable by both financial penalties and jail terms. A study was done from Mzumbe University (Mohamed, 2020) to examine the law and practice regarding patient data privacy and confidentiality. The research investigated how the law governs patient data privacy and confidentiality, and how Tanzania can improve its data privacy laws. However, the study does not explain the current state or the mechanisms used to ensure privacy in EMRs, thereby undermining patient trust. Moreover, without privacy assurances, patients faced the question of whether to disclose information

to healthcare providers to enhance care or withhold it to avoid inappropriate use (McGraw, Dempsey, Harris, & Goldman, 2009).

The literature shows apparent privacy and security weaknesses in existing EMR implementations in Tanzania, alongside a new but still maturing legal framework for personal data protection. It also shows rapid growth in global blockchain-based health privacy frameworks. Yet there is a lack of context-specific designs that bridge these two bodies of work. Existing Tanzanian studies describe fragmented EMR systems, limited privacy awareness and regulatory gaps, while global blockchain research largely ignores the constraints and workflows of Tanzanian public hospitals. No published study identified a blockchain-based framework that specifies, implements, and evaluates a framework that addresses concrete privacy weaknesses in Tanzanian EMRs, aligns with PDPA requirements, and fits within the technical and organisational capacity of government facilities. The proposed framework, Enhancing EMR privacy in Tanzania: A blockchain-based framework, addresses this gap in several ways. First, it is explicitly grounded in the Tanzanian context. The framework maps PDPA principles and the Personal Data Protection Regulations to technical and organisational components of EMR privacy, including consent recording, access control, logging, and breach response, within a permissioned blockchain that links to existing hospital EMRs rather than replacing them. This alignment with Tanzanian law and health information system guidelines distinguishes it from generic blockchain architectures designed for other jurisdictions.

METHODOLOGY

The study population comprised healthcare workers at the Dodoma Region Referral Hospital. The units of analysis were hospital nurses' staff, doctors' staff, ICT staff and patients. Disregarding gender variation, all staff and patients were involved in the study, as they were expected to provide relevant information about the privacy of Electronic Medical Records in Government hospitals in Tanzania. Purposive sampling is based on the researcher's judgment and the study's purpose (Babbie, 1992). The study used this technique because the selected respondents had the characteristics which the researcher needed.

The total population of hospital workers using the EMR system was 442. The research used Stovin's formula to get a sample size of two hundred and ten (210) respondents, who were selected by using a purposeful sampling technique, including hospital staff and patients. The data collection methods used in this study were a questionnaire with closed-ended and

Likert-scale questions, an interview with structured questions. The data were organised, described, coded, and analysed using Statistical Package for the Social Sciences (SPSS) version 25 and EPI Info version 7.1.310 to produce simple descriptive statistics, such as frequency analyses and percentages, and to generate tables and charts for quantitative data. The study employs a questionnaire data collection instrument for clinicians, records staff, and ICT staff. The data were collected on EMR usage, privacy practices, awareness of the PDPA, perceived risks, and views on blockchain-based controls. Key expert interviews were used during framework validations, and thematic analysis was applied to the combined qualitative data from semi-structured interviews and open-ended questionnaire responses. The study focused on privacy rights, experience with the EMR, and the acceptability of patient involvement in a blockchain-based model. The analysis combined descriptive statistics and a user experience test, including scenario-based simulations (e.g., doctor/pharmacist/insurance access requests) and prototype demonstrations with anonymized data, conducted as part of framework validation with experts. Also, it was used to examine how role, experience, and awareness shaped privacy perceptions among EMR users; thematic analysis was applied to combine qualitative data from semi-structured interviews and open-ended questionnaire responses. ICT staff expressed greater concern about weak safeguards, while newer staff had lower confidence in current controls. Awareness of the Personal Data Protection Act, alongside more substantial support for blockchain-based audit trails. Quantitative analysis produced descriptive statistics that supported three themes identified through thematic analysis of qualitative data (interviews and open responses): weak technical safeguards, low awareness of privacy rights, and strong support for transparent access tracking.

RESULTS AND DISCUSSION

The presentation, data analysis, and discussion are sequenced according to the order of the research questions. To achieve the research objectives, the researcher analysed the data systematically and accurately. The data were analysed to achieve the study's objectives.

Results from hospital workers

The data was collected from six different staff members, where nurses (36.1 percent), Doctors (18.5 percent), receptionists (18.5 percent), ICT specialists (13 percent), laboratory technicians (7.4 percent), pharmacists (5.6 percent), and radiologists (0.9 percent), as Table 1 shows.

Table 1:
Respondents' occupation

Occupation	Frequency	Percentage	Cumulative Percentage
Doctor	20	18.5	18.5
Nurse	39	36.1	54.6
Pharmacist	6	5.6	60.2
Laboratory Technician	8	7.4	67.6
Radiologist	1	0.9	68.5
ICT' Specialist	14	13.0	81.5
Receptionist	20	18.5	100.0
Total	**108**	**100.0**	

Note: Percentages sum to 100.0% (minor rounding applied)

The analysis of user experience with Electronic Medical Records (EMR) systems among 108 respondents reveals a notably experienced user base, with half (50.0 percent) reporting more than two years of usage and an additional 42.6 percent having 1 to 2 years of experience, resulting in over 92 percent of users possessing at least one year of familiarity. Only a small proportion (7.4 percent) fall into the novice category of 6 months to 1 year, as shown in Table 2, indicating that the sample largely comprises seasoned EMR users rather than recent adopters. This distribution suggests successful long-term integration of EMR systems in the surveyed setting, likely reflecting sustained usage, effective onboarding for early users, or a workforce with established roles requiring prolonged EMR interaction. The limited presence of short-term users may point to either high retention rates or potential barriers discouraging early-stage participation, highlighting the importance of continued support and advanced feature training to maintain engagement among the predominantly experienced majority while ensuring smoother onboarding for future newcomers.

Table 2:
User experience duration with EMR systems

Experience	Frequency	Percent	Cumulative Percentage
6 months to 1 year	8	7.4	7.4
1 to 2 years	46	42.6	50.0
Above 2 years	54	50.0	100.0
Total	**108**	**100.0**	

Note: Percentages sum to 100.0% (minor rounding applied

The controls taken in the study area to ensure the privacy of electronic data when transferred from one place to another are Password-protected data files without encryption, which account for 75.9 percent, as shown in Table 3.

Table 3:
Privacy controls for transferred electronic data

Privacy controls	Frequency	Percentage	Cumulative percentage
Authentication of the identifiers of the sender and receiver before transfer	7	6.5	6.5
Password-protected data files without encryption	82	75.9	82.4
Encryption of the information during transfer	3	2.8	85.2
post-transfer verification of the appropriate and successful transfer	7	6.5	91.7
Privileged Mode	9	8.3	100.0
Total	**108**	**100.0**	

Note: Percentages sum to 100.0% (minor rounding applied)

However, the findings from the study area show that there were no clearly defined roles and access levels for all staff with authorised access to the patient EMR. As shown in Table 4, staff (72.2 percent) agreed that there were no clearly defined roles or policies for authorised staff to access the patient's information. This shows that the patient's privacy was at high risk.

Table 4:
Clarity of staff roles and access levels for authorized EMR users

Clarity	Frequency	Percentage	Cumulative Percentage
Yes	30	27.8	27.8
No	78	72.2	100.0
Total	108	100.0	

Note: Percentages sum to 100.0% (minor rounding applied)

Results from patients

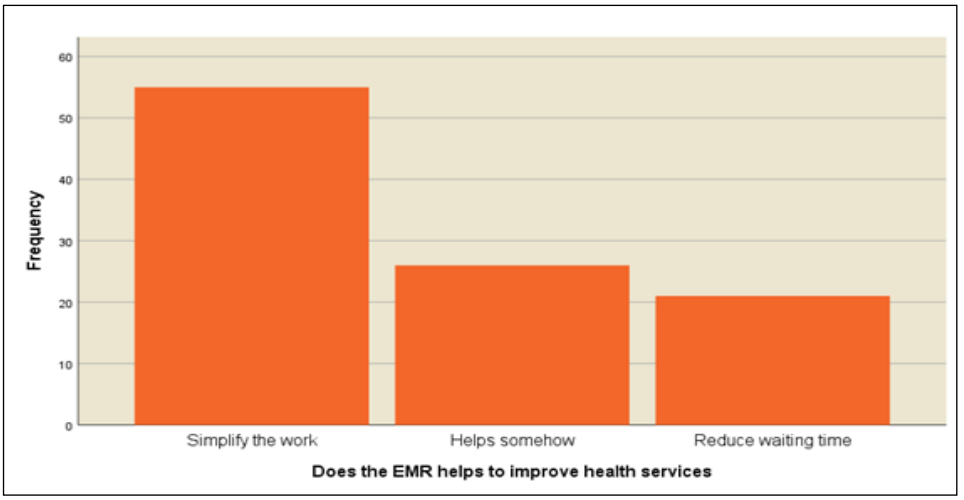
The patient's experience with EMR at government hospitals shows that 85.3 percent of respondents believe EMR is superior to paper records. Specifically, 53.9 percent of respondents say it simplifies their work, 20.6 percent note that it reduces waiting times, and 25.5 percent feel it enhances health services, as illustrated in Table 5 and Figure 2.

Table 5:
Comparison EMR and paper records

	Frequency	Percentage	Cumulative Percentage
Yes	87	85.3	85.3
No	5	4.9	90.2
I am not sure	10	9.8	100.0
Total	102	100.0	

Note: Percentages sum to 100.0% (minor rounding applied)

Figure 1:
Impact of EMR on Health Service Improvement



However, many patients who accessed services at Government hospitals are concerned about the privacy of their health information. As the results show in Table 6, 66 respondents (64.7 percent) concluded that they have worries about the privacy of electronic medical records, since many of them do not have enough knowledge about how the privacy of their medical records is managed electronically.

Table 6:
Concern about the privacy of your EMR

	Frequency	Percentage	Cumulative Percentage
No	36	35.3	35.3
Yes	66	64.7	100.0
Total	102	100.0	

Note: Percentages sum to 100.0% (minor rounding applied)

Technical safeguard regarding EMR privacy

To provide a comprehensive understanding of the finding's, semi-structured interviews were conducted alongside with: one with hospital staff exclusively and the other with a diverse mix of staff and patients. These discussions aimed to explore in greater depth participants' experiences, concerns, and expectations regarding the privacy of electronic medical records (EMRs). Thematic analysis of the qualitative data identified three prominent themes that align with the quantitative results: inadequate technical safeguards, low levels of privacy awareness, and an urgent need for improved accountability within the system. Inadequate Technical Safeguards and Risky Workarounds were consistently highlighted throughout the discussions as significant practical challenges posed by the current EMR system. Many described how these limitations compel staff to resort to unorthodox and potentially dangerous practices, such as sharing passwords, to maintain workflow efficiency. This theme is starkly reflected in the quantitative data, which shows that staff (75.9 percent) depend on password-protected files that lack encryption, as indicated in Table 3, and that respondents (72.2 percent) reported experiencing confusion surrounding access roles, detailed in Table 4, Representative quotes from the interviews are presented to illustrate group consensus; individual semi-structured interview quotes supplement these insights.

> "We share passwords sometimes due to limited access rights. If one person is busy, another has to log in to avoid delaying patient care, there is no other way." Staff Nurse

> "The firewall blocks useful actions we need every day, so people find shortcuts. That creates bigger privacy risks than the firewall was supposed to prevent." ICT Officer

Both patients and some staff reported limited awareness of privacy rights and data management. They had a restricted understanding of how electronic records are stored, protected, or shared, resulting in widespread confusion and anxiety. This finding reinforces the findings of patients (64.7 percent) who reported worries about EMR privacy, as shown in Table 6,

and the generally low awareness of the Personal Data Protection Act observed in the interview, as said by a respondent;

> "I worry about who sees my records; no one explains the system or asks for my consent before anything is entered. "Outpatient (Female)
> "We trust the doctors, but with computers, I don't know if my information stays inside the hospital or goes somewhere else." Patient (Male)

There was strong demand for transparent tracking and patient involvement, with participants consistently calling for improved auditability, real-time access logging, and mechanisms for patients to control, or at least know, who views their data. This strong desire for transparency and accountability directly justifies the proposed blockchain framework's immutable audit trails and consent-based access control features.

> "We really need a system that tracks every access, who opened the record, when, and why. That would build trust for everyone." Doctor
> "If I could see who looked at my file and give permission before sharing it with insurance or another hospital, I would feel much safer." Patient

Thematic analysis of interview transcripts (one staff-only and one mixed staff-patient) confirmed and refined these themes, revealing group consensus on password-sharing workarounds and strong collective support for blockchain-enabled audit trails as solutions to current vulnerabilities. The study identifies a critical intersection between technical vulnerabilities and institutional
gaps in Tanzanian EMR systems, where a heavy reliance on basic, non-encrypted password protection (75.9 percent) and centralized architectures creates significant privacy risks and single points of failure. These technical weaknesses are exacerbated by a lack of clearly defined staff access roles (72.2 percent) and a general lack of awareness of the Personal Data Protection Act (PDPA), leading to shared passwords and weak audit mechanisms that undermine patient trust.

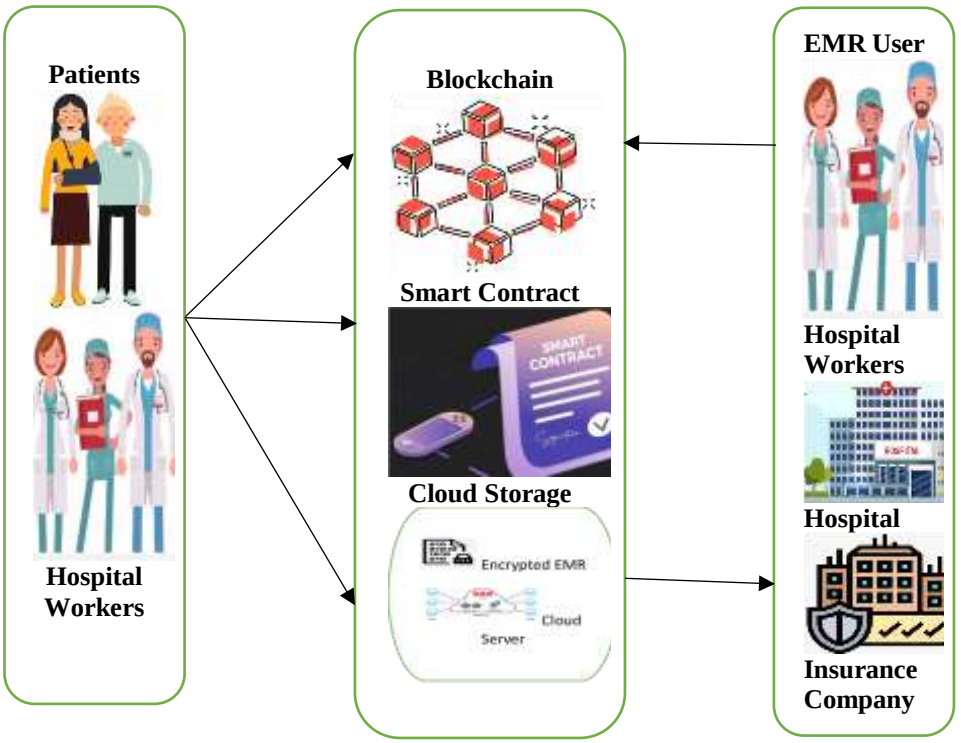
Consequently, patients (64.7 percent) express concern about the privacy of their electronic records. To address these challenges, the research proposes a decentralized blockchain-based framework that utilizes Proxy Re-Encryption (PRE) and smart contracts, which was validated by experts as a feasible solution for transparent access tracking, immutable audit trails, and secure, consent-based data sharing. These thematically derived insights directly informed the design of the proposed blockchain framework, particularly the emphasis on immutable audit trails and consent-based access control via Proxy Re-Encryption (PRE).

Designing an EMR privacy framework for Government hospitals using blockchain technology

The current firewall protects basic traffic but restricts operations, reduces performance, and fails against insider/third-party threats. To address this, the proposed blockchain framework employs Proxy Re-Encryption (PRE) to enable secure, consent-based sharing. The study found that the hospital uses user IDs, passwords, and a Firewall to maintain patient data privacy. A Firewall is a set of components located between two networks that filter traffic between them according to security policies. A Firewall can be an effective means of protecting local systems and networks from network-based security threats while also affording access to the outside world through wide-area networks and the Internet. A weakness of firewalls in privacy protection was that, in practice, they were beneficial for the average user but problematic for large institutions or organisations. The firewall's policies can restrict staff from performing certain operations. This severely affects the overall productivity of the organisations. Sometimes this compels staff to use shortcuts, which can lead to serious privacy problems. However, the use of software firewalls can limit a computer system's overall performance. Therefore, using the firewall method to maintain the patient's EMR privacy may infringe on the patient's privacy whenever any third party, other than hospital workers, attempts to access the patient's data. Given this dilemma, no related research has been conducted on this issue. Therefore, the researcher designed a blockchain framework based on the EMR scheme for data sharing that uses the PRE (Proxy Re-Encryption) technology to enable third-party access to patients' data.

Figure 3 illustrates the operational framework: patients must be registered on the hospital's server before consulting a medical professional. Hospital personnel- including doctors, nurses, pharmacists, and laboratory technicians- generate new blocks and Electronic Medical Records (EMRs) for each patient and subsequently broadcast them to the hospital's private blockchain. The cloud infrastructure securely stores encrypted EMRs uploaded by hospital staff. Third-party entities, such as the National Health Insurance Fund (NHIF), which are system users other than hospital staff, access patients' EMRs. The framework is constructed around an EMR data-sharing scheme utilising Proxy Re-Encryption (pre) technology.

Figure 1:
A designed EMR privacy framework for Government hospitals by using blockchain technology



Validation of the designed framework

Validation involved user experience testing through expert review sessions (resembling structured focus group discussions) with five specialists (ICT officers, cybersecurity expert, records management expert), who assessed the framework via scenario simulations and prototype testing. The framework was validated through a scenario-based expert assessment and a small prototype test using anonymised data. Five specialists, including ICT officers, a cybersecurity expert, and a records management expert, reviewed the structure, access rules, and PRE-based data sharing. They confirmed that the design fits existing EMR workflows and addresses privacy gaps such as shared passwords and a lack of audit trails. A simulation of a doctor, pharmacist and insurance access showed that authorised actions were logged and unauthorised requests were blocked. Experts agreed that the consent feature supports national data protection requirements. The validation shows that the framework is feasible and

acceptable in practice. The following were the results from interview when there is validation of the framework in Hospitals:

> "The use of Proxy Re-Encryption (PRE) is the strongest feature here. It allows the hospital to share data with the National Health Insurance Fund (NHIF) without ever exposing the raw private keys, which solves a major current vulnerability." Cybersecurity Expert

> "From a records management perspective, the immutable audit trail on the blockchain is a game-changer. Currently, we can't prove if a record was tampered with after the fact; this framework makes every edit permanent and visible." Records Management Expert.

> "While the technical design is sound, the challenge will be the 'human element.' If staff continue to share passwords, even a blockchain cannot prevent an authorized user from letting someone else use their terminal." ICT Office

It shows that all experts strongly supported the framework's core technical strengths, highlighting its potential to significantly improve EMR privacy in Tanzanian government hospitals. The Cybersecurity Expert and Records Management Expert highlighted blockchain's advanced cryptographic features, PRE for secure, keyless third-party sharing, and immutable audit trails for tamper-proof logging, viewing these as direct solutions to existing vulnerabilities such as unauthorised access and a lack of traceability. Their opinions align closely, emphasising how these mechanisms enhance data integrity, patient control, and compliance with PDPA, with no noted drawbacks in the technical design itself.

In contrast, the ICT Officer introduced a pragmatic, cautionary perspective by shifting attention to human factors as the primary remaining risk. While acknowledging the design's soundness, they highlighted that technical excellence alone is insufficient if operational behaviors (e.g., password sharing due to workflow pressures or limited training) persist. This contrasts with the more optimistic technical endorsements by underscoring implementation challenges in resource-constrained settings, where user adoption, training, and policy enforcement are critical for real-world success.

Overall, the experts converge on the framework's strong technical feasibility and privacy benefits but diverge in emphasis: two prioritise innovative cryptographic protections as transformative, while the third stresses the need to address socio-technical (human) barriers to ensure long-term effectiveness. This balanced feedback reinforces the

framework's promise and recommends complementary measures, including staff training and access policy reforms.

CONCLUSION AND RECOMMENDATIONS

In this study, the researchers investigated several questions regarding the perceived privacy of electronic medical records in government hospitals. Patients' perceptions of the privacy of their EMR data indicate that many are concerned about its confidentiality due to limited knowledge about how their health data is managed. Not only that, but the privacy techniques and framework used in the study area also help address privacy issues; however, the existing framework does not solve the privacy problem due to specific weaknesses. Therefore, the researcher introduces a blockchain framework to address the existing shortcomings of the framework used in the study area. The study was limited by its geographic scope (a single hospital), time constraints, and the sampling technique used. The researcher suggests specific areas for future research, such as pilot studies testing the blockchain framework across multiple hospitals. Also investigating patient attitudes towards EMR privacy on a larger scale.

Despite patients and users expressing general comfort with Electronic Medical Record (EMR) systems, significant privacy concerns remain that could undermine the accuracy of healthcare data and public trust. To address this, governments, the Ministry of Health, and relevant authorities should urgently implement and enforce robust privacy protection strategies at this early stage, enhance training programs for EMR users (which many respondents found inadequate for safeguarding patient privacy), and ensure healthcare providers transparently inform patients about how their health data is stored and processed. Additionally, patients and system users must be actively involved and empowered before new technologies are adopted to promote greater engagement in their own care. Finally, as this study was limited to government hospitals in a single location over a short period and may not reflect broader privacy issues, further comprehensive research is recommended to evaluate the effectiveness of privacy frameworks and the full benefits and challenges of EMR implementation

REFERENCES

Aina, L. O. (2002). *Research methodologies in information sciences*. Ibadan, Nigeria: Stirling-Holden. ISBN: 978-978-052-327-5

Al-Nassar, B., Abdullah, S., & Osman, W. R. (2009). Barriers for implementation of electronic medical record (EMR). *Journal of Medicine*, 10(2).

Alpert, J. S. (2016). The electronic medical record in 2016: Advantages and disadvantages. *Digital Medicine*, 2(2), 48–51. doi:10.4103/2468-5577.191244, https://doi.org/10.4103/2226-8561.189504

Andriole, K. P. (2014). Security of electronic medical information and patient privacy: What you need to know. *Journal of the American College of Radiology*, 11(12), 1212–1216. https://doi.org/10.1016/j.jacr.2014.09.013

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., & De Caro, A. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. *In Proceedings of the Thirteenth EuroSys Conference* (p. 30). New York, NY: ACM. https://doi.org/10.1145/3190508.3190538

Babbie, E. R. (1992). *The practice of social research.* Belmont, CA: Wadsworth Publishing Company. ISBN: 978-0534159580

Balsari, S., Alexander, F., Joaqun, A. B., Adrian, G., Malavika, J., & Rahul, M. (2018). Reimagining health data exchange: An application programming interface-enabled roadmap for India. *Journal of Medical Internet Research*, 20(7), . https://doi.org/10.2196/10725

Berghel, H. (2017). Equifax and the latest round of identity theft roulette. *Computer,* 50(12), 72–76. https://doi.org/10.1109/MC.2017.4451227

Chali, F., Yonah, Z. O., & Kalegele, K. (2018). Data exchange architecture for the development of mobile applications that support eHealth systems interoperability: A case of Tanzania. *International Journal of Advanced ComputerResearch*,8(34),1-11 https://doi.org/10.19101/IJACR.2018.834006

Choi, Y. B., Capitan, K. E., Krause, J. S., & Streeper, M. M. (2006). Challenges associated with privacy in health care industry. *Journal of Medical Systems*, 30(1), 57–64. https://doi.org/10.1007/s10916-006-7405-0

Daria, S. O., Kok, N., Basoglu, N., & Daim, T. (2019). Adoption factors of electronic health record systems. *Technology in Society*, 58, 101144. https://doi.org/10.1016/j.techsoc.2019.101144

George, J., & Bhila, T. (2019). Security, confidentiality and privacy in health of healthcare data. International *Journal of Trend in Scientific Research and Development*, 3(4), 856–858. https://doi.org/10.31142/ijtsrd23780

Haux, R. (2006). Health information systems – past, present, future. International *Journal of Medical Informatics*, 75(3-4), 268–281. https://doi.org/10.1016/j.ijmedinf.2005.08.002

Hwang, J., & Syamsuddin, I. (2009). Information security policy decision making: An analytic hierarchy process approach. *In Third Asia International Conference on Modelling & Simulatio*n (pp. 158–163). IEEE. https://doi.org/10.1109/AMS.2009.49

Kajirunga, G., & Kalegele, K. (2015). Analysis of activities and operations in the current e-health landscape in Tanzania: Focus on interoperability and collaboration. *International Journal of Computer Science and Information Security*, 13(6), 49–54.

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of Medical Systems*, 41(127). https://doi.org/10.1007/s10916-017-0778-4

Kumar, R. (2015). *Research methodology: A step-by-step guide for beginners* (4th ed.). Thousand Oaks, CA: SAGE Publications. ISBN: 978-1446269688

Lakbala, P., & Dindarloo, K. (2014). Physicians' perception and attitude toward electronic medical record. *Springer Plus,* 3(1), 63. https://doi.org/10.1186/2193-1801-3-63

Lee, L. M. (2017). Ethics and subsequent use of electronic health record data. *Journal of Biomedical Informatics*, 71, 143–146. https://doi.org/10.1016/j.jbi.2017.05.022

Mohamed, H. (2020). Patient's data privacy and confidentiality in Tanzania: *Examination of the law and practice*. Mzumbe University, Morogoro, Tanzania.

Mohurle, S., & Patil, M. (2017). A brief study of WannaCry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5), 1938–1940. https://doi.org/10.26483/ijarcs.v8i5.4021

Munyaradzi, C., Katurura, M., & Cilliers, L. (2018). Electronic health record system in the public health care sector of South Africa: A systematic literature review. *African Journal of Primary Health Care & Family Medicine*, 10(1), 1–8. https://doi.org/10.4102/phcfm.v10i1.1746

Nehemiah, L. (2014). Towards EHR interoperability in Tanzania hospitals: Issues, challenges and opportunities. *International Journal of Computer Science, Engineering and Applications*, 4(4), 21–32. doi:10.5121/ijcsea.2014.4403

Nsaghurwe, A., Dwivedi, V., Ndesanjo, W., Bamsi, H., Busiga, M., & Nyella, E. (2021). One country's journey to interoperability: Tanzania's experience developing and implementing a national health information exchange. *BMC Medical Informatics and*

Decision Making, 21(1), 1–11. https://doi.org/10.1186/s12911-021-01499-6

Ochieng, G. O., & Hosoi, R. (2005). Factors influencing diffusion of electronic medical records: A case study in three healthcare institutions in Japan. *Health Information Management Journal,* 34(4), 120–129. https://doi.org/10.1177/183335830503400405

Odai, E., Zaidan, A. A., Alwi, N. H., Zaidan, B. B., Alsalem, M. A., Albahri, O. S., ... & Albahri, A. S. (2018). Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. *Health and Technology*, 8, 273–287.

Ohno-Machado, L., Silveira, P., & Vinterbo, S. (2004). Protecting patient privacy by quantifiable control of disclosures in disseminated databases. International *Journal of Medical Informatics*, 73(7-8), 599–606. https://doi.org/10.1016/j.ijmedinf.2004.05.002

Pappas, J. A. (2008). *A revitalized information assurance training approach and information* (Master's thesis). Naval Postgraduate School, Monterey, CA.

Sattarova Feruza, Y., & Kim, T. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering,* 2(2), 17–32.

Spigel, L., Samuel, W., & Christina, V. (2018). mHealth data security, privacy, and confidentiality: Guidelines for program implementers and policymakers. Washington, DC: *Health Data Collaborative*.

Thompson, T. G., & Brailer, D. J. (2004*). The decade of health information technology: Delivering consumer-centric and information-rich health care Framework for strategic action*. Washington, DC: U.S. Department of Health and Human Services.

Wang, C. K. (2015). Security and privacy of personal health record, electronic medical record and health information. *Problems and Perspectives in Management*, 13(4), 19–26.

Wanyonyi, E., Rodrigues, A., Abeka, S., & Ogara, S. (2017). Effectiveness of security controls on electronic health records. *International Journal of Science and Technology Research*, 6(12), 170–174.

Wilkowska, W., & Ziefle, M. (2011). Privacy and data security in e-health: The roles of demographic factors and personal traits. *In 5th International Conference on Pervasive Computing Technologies for Healthcare* (pp. 593–600). IEEE. https://doi.org/10.1177/1460458212442933

York, T. W., & MacAlister, D. (2015). *Hospital and healthcare security (6th ed.)*. Oxford, UK: Butterworth-Heinemann. ISBN: 978-0124200487.

.