International Journal of Research in Interdisciplinary Studies
Volume 2, Issue 9, September 2024
https://www.ijris.com | ISSN (Online): 2584-1017

A Critical Review of Information Security and Privacy in Electronic Healthcare Systems: Implications and Future Research for Kenyan Healthcare Systems

Fredrick Ochieng Omogah[1*], Anthony J. Rodrigues[2], Silvance O. Abeka[3]
[1]*Lecturer, Uzima University, Kisumu, Kenya*
[2,3]*Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya*

Abstract— Objectives: The paper aims to critically examine existing literature on information security and privacy challenges in Electronic Healthcare Systems (EHCS) at Jaramogi Oginga Odinga Teaching and Referral Hospital (JOOTRH), Kenya. It evaluates the efficacy of current security protocols and identifies key vulnerabilities, such as unauthorized access and data breaches, in safeguarding patient data. Justification: With the growing prevalence of EHCS and increasing concerns over data security, this review highlights the urgent need to address vulnerabilities in the existing systems. By focusing on under-researched areas like cross-facility data exchange and real-time monitoring, the study underscores the importance of identifying literature gaps to enhance patient data protection in Kenyan healthcare systems. Results: The review identifies critical security threats, such as unauthorized access, data breaches, and insufficient cross-facility data exchange protocols. It also reveals that current frameworks have limitations in addressing these threats and emphasizes the need for improved encryption protocols, better user training, and enhanced collaboration between healthcare facilities and EHCS developers. Conclusion: The findings suggest that there is a pressing need for more robust security measures and collaborative efforts between stakeholders to mitigate security risks in EHCS. This review provides recommendations for healthcare institutions and developers to strengthen electronic health records protection and lays the groundwork for future research to develop a comprehensive information security framework tailored to the challenges in Kenyan and other developing healthcare systems.

***Index Terms*— Electronic Healthcare Systems (EHCS), Information Security and privacy Framework, Data Breaches, Patient Data Protection.**

1. Introduction

Information security and privacy in Electronic Healthcare Systems (EHCS) have become critical concerns, particularly in Kenya, where the adoption of digital healthcare solutions is increasing rapidly. This paper offers a comprehensive literature review of the challenges, existing frameworks, and security vulnerabilities faced by Kenyan EHCS. As the healthcare sector transitions to digital platforms, assessing these systems' ability to protect sensitive patient data from cyber threats is crucial. While digital health advancements have improved healthcare delivery, they also introduce significant challenges related to securing and maintaining patient privacy. These challenges are exacerbated in developing nations with limited resources, awareness, and infrastructure.

To address these issues, this study leverages established theoretical frameworks. Integrated Systems Theory, proposed by Hong et al. (2003), provides a holistic approach to managing information security and privacy, facilitating a comprehensive understanding of EHCS strategies. Complementing this, Contingency Theory, developed by Woodward (1958), emphasizes the need to adapt organizational strategies to environmental conditions. This theory is instrumental in addressing EHCS security and privacy issues by considering situational factors such as infrastructure and resource availability. By integrating these frameworks, this study aims to enhance the effectiveness of EHCS in safeguarding sensitive patient information within diverse contexts.

2. Current Security and Privacy Situations of Patients' Information

Information security and privacy are crucial for maintaining patient trust and effective healthcare delivery. In Kenya, the adoption of Electronic Healthcare Systems (EHCS) has introduced both opportunities and challenges in managing patient data. The effectiveness of these systems in safeguarding sensitive patient information is increasingly important as digital health solutions become more prevalent. The COVID-19 pandemic has underscored vulnerabilities in global healthcare systems, including Kenya's. The pandemic heightened fears of stigma and discrimination related to health status, leading to patients being hesitant to disclose their condition. This reluctance impacted public health responses and data management (Health Privacy Project, 2007).

The shift from manual to electronic health records (EHRs) has improved data management and accessibility but also

*Corresponding author: fo2001ke@yahoo.com

introduced significant security and privacy risks. Data breaches have become a major concern, with inadequate security measures exposing patients to economic and social harm. For example, a U.S. survey found that 75% of patients are concerned about unauthorized information sharing by health websites (Raman, 2007). This highlights the urgent need for robust security measures (Hasan & Yurcik, 2006). Despite technological advancements, research on information security and privacy in healthcare remains limited. While interdisciplinary studies have explored security risks and governance, there is a notable gap in research addressing the unique challenges of healthcare information security.

In Kenya, the implementation of Electronic Medical Records (EMRs) has raised new security and privacy concerns. Systems like MMRS, Open MRS, and Kenya EMR are in use, but issues such as inadequate e-legislation and standards persist (Mugo & Nzuki, 2014). The absence of comprehensive e-health legislation exacerbates these concerns, potentially undermining patient confidence in these systems.

Globally, increased data sharing and connectivity present both benefits and risks. In Africa, including Kenya, challenges such as insufficient cybersecurity research, lack of awareness and inadequate legal and technical measures complicate patient data protection (Kritzinger & Solmns, 2012). The lack of basic cybersecurity knowledge among a significant portion of the population further exacerbates these issues. Research on EHRs in developing countries indicates challenges like equipment failures and inadequate technical expertise (Sood et al., 2008). The connection of EHR systems to the internet also poses risks of unauthorized access, as shown by a data breach in South Africa involving a public figure's health records (Adesina et al., 2011).

Addressing these security and privacy challenges in Electronic Healthcare Systems is essential for effective healthcare delivery in Kenya. While digital records offer benefits, they also introduce risks that require comprehensive research and robust frameworks to ensure patient information is protected and trust in digital health systems is maintained.

3. Electronic Healthcare's Security and Privacy Frameworks

Over the past 40 years, the U.S. healthcare industry has undergone significant changes driven by advancements in IT and legislation like HIPAA. HIPAA's Privacy and Security Rules mandate safeguards to protect patient information. As healthcare data becomes increasingly digital, new privacy risks emerge, necessitating stronger security measures to protect sensitive information (Choi et al., 2006; Mercuri, 2004). The U.S. Congress has proposed regulations like the Health Information Privacy and Security Act and the National Health IT and Privacy Advancement Act of 2007 to enhance privacy protections by incentivizing de-identification and improving health IT systems (USC, 2007a, 2007b). Research highlights security issues such as its impact on medical errors, access control design, and data interoperability (Dhillon & Backhouse, 2001).

In developing countries like Kenya, implementing Electronic Medical Records (EMRs) presents challenges. A study in the Journal of Innovation in Implementing Health Informatics in Primary Care highlights the need for data quality, user-friendly systems, and training in areas with limited computer literacy. Structured data simplifies verification, though valuable unstructured data may be lost (Hevner et al., 2004).

Securing patient data is a critical concern in developing regions. Effective protection includes technical and human protocols, such as complex passwords, restricted access, encryption, and physical security (Fraser et al., 2005). Healey (2008) notes that successful e-health implementation requires overcoming infrastructure, political, and resource challenges, offering benefits like improved data management and better tracking of health conditions such as HIV and MDR-TB.

In summary, establishing strong security and privacy frameworks for Electronic Healthcare Systems (EHCS) is vital to ensuring effective healthcare delivery in Kenya. Comprehensive research and well-developed frameworks are critical for safeguarding patient information and fostering trust in digital health systems. As healthcare technology advances, balancing innovation with robust security measures will be essential for the successful implementation of EHCS.

4. Information Security Frameworks

A. ISO/IEC 27001 Framework

ISO/IEC 27001 is an international standard for information security management systems (ISMS). The latest update was in 2017. It helps organizations identify and manage security risks, build trust with stakeholders, and secure information assets including employee details, intellectual property, and financial information.

B. The NIST Cybersecurity Framework

Developed by the US National Institute of Standards and Technology (NIST), this framework provides guidelines for cybersecurity maturity through a common language. Its framework Core includes activities and desired results categorized into five functions: Identify, Protect, Detect, Respond, and Recover. It offers insights into an organization's approach to cybersecurity risk management. The framework Profiles tailor an organization's requirements, objectives, risk tolerance, and resources with the outcomes of the Framework Core. The core Functions are

- *Identification:* Asset management, risk assessment, and supply chain risk management.
- *Protection:* Identity management, data security, and protective technologies.
- *Detection:* Continuous monitoring and detection processes.
- *Response:* Respond planning and communication.
- *Recover:* Recovery plans and improvements.

The recent developments indicate that NIST has proposed new frameworks addressing the intersection of cybersecurity, data security, and privacy.

C. COBIT

Control Objectives for Information and related Technology (COBIT), is a governance framework by ISACA. COBIT 5 for Information Security integrates governance with management, focusing on achieving benefits while managing risks. Key aspects of COBIT and principles are to define enable and Optimize resource use, considering enterprise and stakeholder benefits for effective governance and management.

D. Reliability Framework for Enhancing Health Data Security and Privacy

This emphasizes on regular updates and backups of healthcare data. The backup Strategy ensures maintenance of at least three copies of backup on two different media, with one stored offsite. Storage options involves the use of CD/USB, hard disks, and online storage (e.g., OneDrive, Google Drive, Dropbox) to ensure data security and availability.

E. Organizational Control Framework for Enhancing Security and Privacy

This focuses on organizing and managing security and privacy of health data within healthcare centers. Major components in place are

- *Organizational Structure:* Ensure departments are aware of and adhere to security protocols.
- *Risk Management:* Develop plans to address risks such as data leakage and medical errors.
- *Budget Allocation:* Allocate funds for ICT infrastructure and staff training.
- *Training and Awareness:* Continuous training for employees on new technologies and security practices.

Each framework offers different approaches and focuses, providing a comprehensive set of tools and guidelines for managing information security effectively.

5. Information Privacy Frameworks

Healthcare systems require robust privacy frameworks to protect sensitive patient information while ensuring accessibility for authorized healthcare providers. This section examines key privacy frameworks relevant to Electronic Healthcare Systems (EHCS).

A. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA, established in 1996, aims to standardize electronic health transactions while safeguarding patient privacy. It mandates specific regulations for electronic transactions, privacy, national identifiers, and security rules. These standards are pivotal in ensuring the confidentiality and security of individually identifiable health information within healthcare institutions.

B. The PACT Data Privacy Trust Framework

The PACT framework, introduced by Debbie Reynolds in 2022, focuses on evaluating both regulatory and business risks while building trust concerning data privacy. It consists of four primary components:

Purpose: Clearly defining the data's intended use to establish trust.

Alignment: Ensuring data use aligns with the stated purpose to maintain integrity.

Context: Data usage should be consistent with the context in which it was originally collected, with clear benefits to individuals.

Transparency: Upholding transparency throughout the data lifecycle, ensuring users understand how their data is handled.

C. Access Control Framework

Developed by Shirtwai (2019), the Access Control Framework is integral to managing who has access to healthcare data. It emphasizes the following components:

Access Privileges: Defining and regulating different levels of access based on user roles.

Authorization Accessibility: Ensuring access is granted according to predefined roles and responsibilities.

Availability: Maintaining data accessibility while upholding stringent security controls.

Training: Educating staff on access control policies to enhance security awareness.

D. Encryption Framework

The Encryption Framework, based on Stamp's (2006) work, is a vital aspect of safeguarding health data by encrypting sensitive information. The key components include:

- *Integrity:* Ensuring data remains unaltered during transmission.
- *Confidentiality:* Preventing unauthorized interception or disclosure of data.
- *Authentication:* Verifying the identity of parties involved in data transmission to prevent falsification.
- *Non-repudiation:* Guaranteeing that parties cannot deny their involvement in a communication or transaction.

6. Testing and Validation of EHCS Security Frameworks

The frameworks governing the security and privacy of EHCS require regular testing and validation to ensure compliance and efficacy in protecting sensitive health data. HIPAA Security Rule enforces administrative, physical, and organizational safeguards to protect electronic Protected Health Information (ePHI). Compliance with this rule includes regular updates, security audits, and adherence to written policies. Encryption plays a crucial role in securing data against unauthorized access, both during transmission and storage. Comprehensive cybersecurity strategies are essential for protecting Electronic Health Records (EHRs) from cyber threats, ensuring the security of ePHI across networks. Communication ensuring secure communication channels for transmitting ePHI is critical to prevent data breaches, in compliance with the HIPAA Security Rule.

A. Proposed Integrated Security and Privacy Framework

The conceptual framework proposed in this study aims to achieve high levels of security and privacy for patient

information in EHCS by integrating various independent and intervening variables:

- *Independent Variables:* These include Access Control, Reliability & Backup, Encryption, Organizational Controls, and Shared Information.
- *Intervening Variables:* Factors such as Awareness & Training, Technology Integration, Risk Management, Compliance Behavior, and Incident Response play a mediating role.
- *Dependent Variable:* The goal is to develop an Integrated Information Privacy and Security framework for EHCS.

7. Materials and Methods

This study employed a descriptive cross-sectional design to identify security challenges affecting patients' electronic medical data at Jaramogi Oginga Odinga Teaching and Referral Hospital (JOOTRH) and its associated healthcare facilities in Kisumu County, Kenya. The research targeted over five million patients from more than ten counties in Western Kenya. Using purposive sampling, the study gathered data from 50 respondents, including healthcare administrators, medical staff, IT personnel, and affected patients, with 44 completed questionnaires analyzed. Data collection involved structured questionnaires, interviews, and document analysis, conducted over one month, with strict adherence to ethical standards, including informed consent and COVID-19 prevention measures. Validity was confirmed through convergent and discriminant validity analyses, while reliability was ensured through a test-retest procedure. Data was cleaned, coded, and analyzed using SPSS Version 25.0 and Excel 2010.

8. Findings and Summary of the Research Gap

This literature review highlights the critical security and privacy challenges faced by Electronic Healthcare Systems (EHCS), especially in Kenya. It identifies key vulnerabilities such as unauthorized access, data breaches, and inadequate cross-facility data exchange protocols. Existing frameworks, including HIPAA, encryption models, and access control frameworks, provide foundational measures but are insufficient for addressing the unique needs of developing countries with limited resources and infrastructure. The review underscores the need for advanced encryption, improved user training, and enhanced collaboration between healthcare facilities and system developers to address these gaps effectively.

A. Research Gaps

Integrated Framework Development: There is a notable gap in the development of a comprehensive framework that integrates both security and privacy concerns, specifically tailored for the unique challenges faced by EHCS in Kenya.

User Training: The current research lacks in-depth studies on effective user training programs for EHCS, highlighting a need for targeted training strategies that address emerging security threats and best practices.

Collaboration Mechanisms: Research does not sufficiently explore how to strengthen collaboration between healthcare facilities, EHCS developers, and regulatory bodies to enhance security protocols and system resilience.

Real-Time Monitoring Solutions: There is a gap in research on innovative real-time monitoring solutions that can detect and respond to security breaches, especially within the context of local infrastructure and resource limitations.

Context-Specific Challenges: Existing studies often overlook the specific challenges posed by limited resources and infrastructure in developing countries, necessitating research that addresses these contextual constraints effectively.

Addressing these research gaps can lead to the development of more effective EHCS frameworks, improving data security and healthcare delivery in developing regions.

9. Conclusion

This literature review has underscored the critical security and privacy challenges facing Electronic Healthcare Systems (EHCS), with a particular focus on the Kenyan context. The review reveals significant vulnerabilities such as unauthorized access, data breaches, and insufficient protocols for cross-facility data exchange. Although existing frameworks, including HIPAA and various encryption and access control models, provide foundational security measures, they fall short in addressing the specific needs of developing countries with limited resources and infrastructure. The gaps in these frameworks highlight the need for enhanced encryption protocols, improved user training, and stronger collaboration between healthcare facilities and system developers.

10. Recommendations

1. *Develop a Comprehensive Integrated Framework:* Future research should focus on creating an integrated security and privacy framework that addresses both privacy and security concerns simultaneously. This framework should be tailored to the unique needs of EHCS in Kenya, incorporating advanced encryption techniques and robust access control mechanisms.
2. *Enhance User Training Programs:* There is a pressing need for improved training programs for users of EHCS. Training should focus on data protection best practices and awareness of emerging security threats to better safeguard patient information.
3. *Strengthen Collaboration:* Foster stronger collaboration between healthcare facilities, EHCS developers, and regulatory bodies. This collaboration should aim to develop and implement more effective security protocols and ensure that the systems are resilient to potential cyber threats.
4. *Innovate Real-Time Monitoring Solutions:* Research should explore innovative solutions for real-time monitoring of EHCS to detect and respond to security breaches promptly. This includes developing tools and methodologies suited to the local infrastructure and resource limitations.
5. *Address Local Context Challenges:* Future studies should consider the specific challenges posed by limited resources and infrastructure in developing countries. Tailoring

solutions to these constraints will be crucial in enhancing the overall effectiveness of EHCS and improving patient data protection.

By addressing these recommendations, future research can contribute to more robust and effective EHCS frameworks, ultimately enhancing patient data security and improving healthcare delivery in developing regions.

Dedication

This study is first and foremost dedicated to *Almighty God* our Creator and to the Blessed Virgin Mary Mother of God and Our Mother Help of the Sick, all His holy Angels and Saints, particularly St. Albert the Patron of Medical Technologies & Scientists. To Abbot Francis Pfanner (1825-1909) - Founder of the Missionary Sisters of Precious Blood & Mariannhill Missionaries ("So run that you may obtain the prize!"). To my late grandparents Anna Mumia Olumo Skingi (Bomb), Johannes Omogah & Orwako (Manwar). Rosalia Abiero (King Nyar Oyengo) & Pius Odera (Nyanjore). To our late Mother Calsine Aketch Omoga for her love, care, and vision towards education and personal growth for us her children. Late Great Aunties Leonora (Odhiambo Range & Gertrude Awuor Nyi'Omogah). Late Great Uncle and Aunt John David Ochino & Grace Ochino respectively, late god father Agustino Keya, late brothers Julius, Peter, Joachim and Raphael, To my beloved wife Elizabeth Nekesa and my children namely Gladwell, Gloria Christa, Gregory and Gerry Jerome, late daughters Claudia and Geraldine. To my dad Pius Omoga, my sister Rose and Brothers Paul Omogah, Richard and Erick for their continued encouragement and support during my studies.

Acknowledgement

I would like to express my gratitude first to *Almighty God* Our Father in Heaven, for His many graces and great care for me up to this far**.** My appreciation and sincere thanks to my supervisors Prof. Anthony J. Rodrigues and Prof. Silvance O. Abeka for your great supervisions, continuous assistance, encouragement, great inspiration, mentorship and guidance throughout my studies. Further appreciation to Prof. Solomon Ogara my lecturer and Director-ICT at JOOUST, Prof. George Raburu (late), Prof. Samuel Liyala, Prof. Tibs and Dr. Jasper Ondulo for their contribution during my studies. I cannot forget my Statistician Linda Odhiambo and my colleagues at work Maurice Onywera, Dannis Oduor Wanda, Kevin Otieno and Henry Christian who assisted in proofreading and fine-tuning my work, and my classmates for moral support.

References

[1] Adesina, A., et al. (2011). Data breach and its implications: A case study from South Africa. *Information Management & Computer Security*.

[2] Choi, N., Kim, D., & Goo, J. (2006). Managerial Information Security Awareness' Impact on an Organization's Information Security Performance. AMCIS 2006 Proceedings, 406.

[3] Dhillon, G., & Backhouse, J. (2001). Current Directions in IS Security Research: Towards Socio- Organizational Perspectives. *Information Systems Journal*, *11*(2), 127–153.

[4] Fraser, H., Biondich, P., Moodley, D., Choi, S., Mamlin, B., & Szolovits, P. (2005). Implementing electronic medical record systems in developing countries. *Journal of Innovations in Health Informatics*, *13*(2), 83–95.

[5] Healey, N. M. (2008). Is higher education in really 'internationalising'? Higher education, 55, 333-355.

[6] Hasan, R., and Yurcik, W. (2006). A Statistical Analysis of Disclosed Storage Security Breaches. *ACM Workshop on Storage Security and Survivability*.

[7] Hevner, A., March, S.T., Park, J., and Ram, S. (2004). Design Science Research in Information Systems. *MIS Quarterly*, *MIS Quarte* (1), 75–106.

[8] Hong, K.S., Chi, Y. P., Chao, L. R., and Tang, J.-H. (2003). An integrated system theory of information security management. Information Management & Computer Security, 11(5), 243–248.

[9] Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers and Security*, *29*(8), 840–847.

[10] Mugo, David M., and David Nzuki. (2014). "Determinants of electronic health in developing countries."

[11] Mercuri, R. T. (2004). The HIPAA-potamus in Health Care Data Security. *Communications of the ACM*, *47*(7).

[12] Omogah, F. O., Rodrigues, A. J., & Abeka, S. O. (2024). A Critical Review of Information Security and Privacy in Electronic Healthcare Systems: Implications and Future Research for Kenyan Healthcare Systems. Uzima University, Jaramogi Oginga Odinga University of Science & Technology (JOOUST), Kenya.

[13] Raman, A. (2007). Enforcing Privacy through Security in Remote Patient Monitoring Ecosystems. *International Special Topic Conference on Information Technology Applications in Biomedicine 6th*, 116.

[14] Sood, S. P., Nwabueze, S. N., Mbarika, V. W., Prakash, N., Chatterjee, S., Ray, P., & Mishra, S. (2008, January). Electronic medical records: A review comparing the challenges in developed and developing countries. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008) (pp. 248-248). IEEE.

[15] Woodward, J. (1958). Contingency Theory and its Application to Information Security. *Management and Technology*. London: Her Majesty's Stationery Office.