Margaret Afwande, 2024, 12:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Assessing Data Security of Patient Health Information in EHMS at Kenyan Public Hospitals

Margaret Afwande[1], Jane Kabo[2], Samuel Barasa[3]
Department of Information Technology, Kibabii University/Bungoma, Kenya[1,3]
School of Nursing, Kibabii University/Bungoma[2]

Abstract- This study explores the cybersecurity vulnerabilities of Electronic Health Management Systems (EHMS) in Kenya's public hospitals, revealing significant shortcomings in the protection of sensitive patient health information. Despite the widespread implementation of EHMS, findings indicate that existing security measures are insufficient to address the escalating cyber threats faced by healthcare institutions. Notably, 78% of hospitals rely solely on username and password authentication, while only 34% have adopted multi-factor authentication (MFA), leaving systems exposed to unauthorized access. Furthermore, just 41% of hospitals encrypt data at rest, highlighting a critical gap in data security. The research identifies alarming trends in unauthorized access incidents, with 60% of respondents reporting such breaches primarily due to weak password practices and a lack of staff training in cybersecurity. Additionally, 80% of respondents cite chronic underfunding as a significant barrier to improving EHMS security. The shortage of skilled IT personnel (68%) and inadequate cybersecurity training for healthcare staff (72%) further exacerbate these vulnerabilities, increasing the risk of data breaches and ransomware attacks. To mitigate these challenges, the study recommends adopting a proactive cybersecurity strategy focused on implementing MFA, comprehensive data encryption, and regular system audits. Furthermore, investment in capacity-building initiatives for IT professionals is essential to strengthen the cybersecurity framework within public hospitals. Establishing a national framework for data security is also crucial for standardizing practices and enhancing patient data protection across Kenya's healthcare sector. Overall, these measures aim to address vulnerabilities and ensure the integrity of sensitive health information in an increasingly digital landscape.

Keywords- Electronic Health Management Systems, Data Security, Kenya Healthcare System, Cyber Threats Patient Health Information

I. INTRODUCTION

The digitization of healthcare systems has led to the widespread adoption of Electronic Health Management Systems (EHMS) in many countries, including Kenya. EHMS have significantly improved healthcare delivery by streamlining patient data management, reducing paperwork, and enabling faster access to critical health information (World Health Organization [WHO], 2022). In Kenya's public hospitals, EHMS have become vital tools in managing patient care, tracking medical histories, and facilitating information sharing among healthcare providers (Ministry of Health, 2021). However, with these advancements comes a heightened concern for the security of sensitive

patient health information (Kimani, Muthoni, & Ndegwa, 2023).

The storage and transmission of patient data through digital systems expose it to a variety of cybersecurity threats, including unauthorized access, data breaches, hacking, and ransomware attacks (Muli, 2022). Healthcare data is particularly vulnerable due to its highly sensitive nature, often containing personal identification information, medical histories, and other confidential details (Ouma, 2021). A breach of such data can result in significant privacy violations, financial fraud, and loss of trust in healthcare institutions (Kimani et al., 2023). In Kenya, recent reports have highlighted the growing incidence of data security breaches in public hospitals, raising questions about the adequacy of current security measures to protect patient health information (Ministry of Health, 2021).

Despite the recognized risks, there is limited research on the state of data security within Kenya's public healthcare sector (Ouma, 2021). Public hospitals, which often operate with limited resources, face additional challenges in implementing robust cybersecurity measures. Factors such as outdated technology underfunded IT departments, and a shortage of skilled personnel exacerbate these security vulnerabilities (WHO, 2022). Given the increasing reliance on EHMS and the critical nature of healthcare data, it is essential to evaluate the current security landscape to identify gaps and recommend strategies for improvement (Muli, 2022).

II. PROBLEM STATEMENT

The adoption of Electronic Health Management Systems (EHMS) in Kenya's public hospitals has streamlined patient data management, improving healthcare delivery. However, this increased reliance on digital systems has also introduced significant risks related to data security, such as unauthorized access and data breaches. Despite the critical nature of patient information, there is limited research on the effectiveness of existing cybersecurity measures within Kenya's public healthcare sector.

This study aims to address this gap by evaluating the current state of EHMS security in public hospitals, identifying common vulnerabilities, and exploring the challenges in protecting patient data. The findings will inform strategies for strengthening data security in resource-constrained environments.

III. RELATED STUDIES

The rapid digitization of healthcare systems globally has brought significant advancements and challenges, particularly concerning the security of patient health information. This literature review examines the current landscape of Electronic Health Management Systems (EHMS), data security concerns related to these systems, the specific context of public hospitals in low- and middle-income countries (LMICs) like Kenya, and proposed frameworks and strategies to enhance data security within healthcare systems.

Electronic Health Management Systems (EHMS) are digital platforms utilized for the collection, storage, management, and exchange of patient health information. These systems are crucial for modern healthcare delivery, as they improve data accessibility, reduce medical errors, and facilitate better coordination among healthcare providers (Sittig & Singh, 2016). However, the increasing reliance on digital records has rendered the healthcare sector a prime target for cybercriminals, given the sensitive nature of health information. Data security within EHMS is a critical concern; breaches can lead to severe consequences, including financial losses, privacy violations, and harm to patient trust (Kruse et al., 2017). Inadequate security measures can result in unauthorized access and theft of sensitive information, exacerbated by evolving cyber threats employing sophisticated methods such as phishing and ransomware (Verma & Raman, 2019).

While EHMS is widely adopted in high-income countries, LMICs, including Kenya, face unique challenges in securing digital health information. Public hospitals in LMICs often lack adequate

resources, infrastructure, and expertise to maintain robust data security systems (Miller et al., 2020). In Kenya, the drive for EHMS adoption has been motivated by the need to enhance healthcare service delivery; however, security remains a critical concern. Many public hospitals rely on outdated software lacking the necessary updates to defend against modern cyber threats. Limited financial resources and insufficient IT personnel further hinder efforts to bolster data security (Muiruri & Wanyoike, 2019). Public hospitals often prioritize basic healthcare services over IT investments, leaving EHMS vulnerable to cyberattacks. Moreover, healthcare workers frequently lack training in cybersecurity practices, heightening the risk of insider threats and accidental data breaches (Were et al., 2020).

Research highlights several prevalent security threats facing EHMS in healthcare institutions. Unauthorized access often results from unauthorized personnel accessing sensitive health records due to weak passwords, lack of multi-factor authentication, and inadequate access controls (Kruse et al., 2017). Ransomware attacks, which involve malicious software encrypting data and demanding payment for release, pose a significant threat, particularly in healthcare settings where operational downtime can have dire consequences (Chinthapalli, 2017). Insider threats also represent a major security risk; employees, whether disgruntled or negligent, can compromise data security. Poor security awareness and inadequate training contribute to the prevalence of these threats. In Kenya, the increasing frequency of ransomware attacks targeting healthcare facilities emphasizes the urgent need for enhanced cybersecurity measures (Oduor & Wanyeki, 2021).

Securing EHMS in public hospitals in developing countries like Kenya involves numerous challenges. Resource limitations represent a primary barrier; public hospitals often operate with constrained budgets, hindering investments in advanced cybersecurity technologies (Akhlaq et al., 2016). Technical challenges, such as reliance on legacy systems with outdated security features, further expose these facilities to cyber threats (Muiruri & Wanyoike, 2019). Additionally, the shortage of trained cybersecurity professionals leaves systems vulnerable to internal and external threats (Were et al., 2020). Organizational challenges, including insufficient cybersecurity policies, lack of enforcement, and inadequate training for healthcare workers, exacerbate the poor state of EHMS security. Many staff members lack the awareness and technical knowledge necessary to protect against cyber threats (Mbugua et al., 2021; Kebaso, 2021).

To address growing concerns over EHMS data security, several frameworks and strategies have been proposed in the literature. A multi-layered security approach incorporating encryption, robust access control mechanisms, and regular system audits is essential for protecting healthcare data (Bhuyan et al., 2020). Encryption ensures data remains unreadable without appropriate decryption keys, while strong access controls prevent unauthorized access to sensitive records (Alharthi et al., 2019). Staff training and awareness programs are critical in mitigating insider threats and preventing accidental data breaches. In Kenya, investing in regular cybersecurity training for hospital staff could significantly reduce human errors leading to security breaches (Gordon et al., 2021). Developing comprehensive data protection policies that outline procedures for data access, handling, and sharing is also vital (Cohen & Mello, 2018).

IV. RESULTS INTERPRETATION AND DISCUSSION

The data collected from IT staff and hospital administrators in Kenya's public hospitals provides critical insights into the current state of electronic health management systems (EHMS) security. The findings reveal that while basic security measures are present, they are inadequate for addressing the comprehensive range of cyber threats that the healthcare sector faces.

Security Measures in Place

The survey results indicate that access controls in most hospitals rely primarily on username and

password authentication, with 78% of respondents affirming this practice. However, only 34% of respondents have implemented multi-factor authentication (MFA) to bolster security. This finding suggests that hospitals are missing a crucial opportunity to enhance their security posture, particularly given the increasing incidence of unauthorized access. MFA can provide an additional verification layer, significantly reducing the chances of unauthorized access due to compromised credentials (Alavi & Keshavarz, 2023).

Encryption practices also show significant room for improvement. Although 56% of hospitals reported implementing encryption for data in transit, only 41% encrypt data at rest. This gap is concerning as unencrypted stored data is particularly vulnerable to breaches, which can expose sensitive patient information. Research has demonstrated that encrypting data at rest can mitigate the impact of data breaches, as encrypted data remains unreadable without the appropriate keys (Raghavan & Menon, 2022). Moreover, regular system audits, essential for identifying vulnerabilities and ensuring compliance with security policies, were conducted by only 42% of hospitals, with the majority performing audits sporadically. This reactive approach, often triggered by prior incidents, underscores a critical weakness in proactive security management.

Common Vulnerabilities and Incidents

The survey revealed that 60% of respondents acknowledged incidents of unauthorized access, predominantly attributed to weak password practices and the lack of MFA. Additionally, 48% of hospitals reported data breaches in the past two years, primarily due to malware attacks, phishing attempts, or internal breaches by disgruntled employees. These statistics highlight the urgent need for robust security measures to counteract the growing sophistication of cyber threats. Ransomware attacks are particularly alarming, with 26% of respondents reporting incidents where patient data was held hostage. The challenges in data recovery due to inadequate backup systems further compound the risk associated with such attacks, emphasizing the importance of having reliable backup and recovery strategies in place (Smith & Chen, 2023).

Challenges in Enhancing EHMS Security

The challenges identified in improving EHMS security are multifaceted. A staggering 80% of respondents cited underfunding as the primary barrier to upgrading security infrastructure. Many public hospitals operate under tight budgets, which often prioritize immediate healthcare needs over cybersecurity investments. The shortage of skilled IT personnel (68% of respondents) and inadequate training for healthcare workers (72% reported lacking formal cybersecurity training) further exacerbate these vulnerabilities. The lack of trained personnel increases the risk of human error, which remains one of the leading causes of security breaches (Jones, Smith, & Kumar, 2024).

Discussions

The results of this study reveal significant security gaps in the management of patient health information within EHMS across Kenya's public hospitals. Despite the presence of fundamental security measures, such as password authentication and data encryption, these measures fall short of addressing the comprehensive threats posed by cybercriminals.

Inadequate access controls represent a major vulnerability. The reliance on basic username and password authentication leaves systems exposed to unauthorized access. The limited adoption of MFA signals a need for hospitals to recognize the increasing risks associated with inadequate access controls. Encryption gaps further highlight the critical vulnerabilities in data management. The disparity between encryption for data in transit and data at rest is concerning, as unencrypted stored data increases the risk of exposure during a breach. Given the sensitivity of patient data, hospitals must prioritize comprehensive encryption strategies to safeguard all data types.

Moreover, the infrequent performance of system audits and testing is a significant oversight. Regular system audits and rigorous testing of backup systems are vital for identifying and addressing

vulnerabilities. The current sporadic approach leaves hospitals at risk of significant data loss and operational disruptions. Addressing these vulnerabilities also requires overcoming resource and staffing constraints. The shortage of skilled IT personnel, coupled with limited funding, presents substantial barriers to enhancing EHMS security. Many public hospitals in Kenya operate on tight budgets, which often deprioritize investments in cybersecurity infrastructure.

To effectively mitigate these vulnerabilities, public hospitals must adopt a proactive cybersecurity strategy. Implementing stronger access control measures, such as MFA, and encrypting all sensitive patient data should be prioritized. Additionally, increasing the frequency of audits and training healthcare staff on cybersecurity will be crucial in reducing human errors that lead to breaches. Addressing these challenges requires a collective effort from both the government and healthcare institutions. Exploring public-private partnerships for funding cybersecurity initiatives and developing capacity-building programs to train IT professionals are critical steps in bolstering EHMS security. Additionally, establishing a national framework for data security in public healthcare can standardize practices and ensure compliance across hospitals, ultimately enhancing patient data security across the sector.

V. CONCLUSION

This study highlights the pressing need for enhanced cybersecurity measures within Electronic Health Management Systems (EHMS) in Kenya's public hospitals. While the digitization of healthcare has streamlined patient data management and improved healthcare delivery, it has also introduced significant vulnerabilities, exposing sensitive health information to cyber threats. The findings reveal that basic security measures are insufficient, with a predominant reliance on username and password authentication and a concerning lack of multi-factor authentication. The inadequate encryption practices, particularly for data at rest, further compound these vulnerabilities, leaving patient information at risk.

Moreover, the study underscores the multifaceted challenges public hospitals face in enhancing EHMS security, including chronic underfunding, a shortage of skilled IT personnel, and insufficient training for healthcare workers. These factors contribute to a heightened risk of unauthorized access and data breaches, further exacerbated by the evolving landscape of cyber threats. The reported incidents of ransomware attacks and other malicious activities emphasize the urgency for hospitals to adopt a more proactive and comprehensive cybersecurity strategy.

To effectively safeguard patient health information, public hospitals must prioritize the implementation of robust access control measures, including multi-factor authentication and comprehensive data encryption. Regular system audits and rigorous staff training are essential components in mitigating insider threats and reducing the likelihood of human errors leading to security breaches. Furthermore, collaborative efforts between government bodies and healthcare institutions are critical in addressing resource constraints and enhancing cybersecurity infrastructure. Establishing a national framework for data security can standardize practices across public hospitals, ensuring compliance and ultimately bolstering patient data security. As Kenya continues to advance in digital healthcare, prioritizing the security of electronic health management systems is not just beneficial—it is imperative for maintaining trust and safeguarding patient welfare in the healthcare sector.

REFERENCES

1. Akhlaq, A., Awais, M., & Zafar, H. (2016). Challenges in adopting electronic health record systems in low and middle-income countries: A systematic review. Health Information Management Journal, 45(4), 184-190.
2. Alavi, S., & Keshavarz, M. (2023). The impact of multi-factor authentication on the security of health information systems. Journal of Cybersecurity and Privacy, 5(1), 45-62.
3. Alharthi, A., Alrahab, H., & Hossain, M. (2019). Data security and privacy in electronic health

record systems: A survey. Health Informatics Journal, 25(3), 1029-1045.
4. Bhuyan, H., Dey, N., & Kharat, A. (2020). A review of the security challenges and solutions for electronic health record systems. Journal of King Saud University - Computer and Information Sciences, 34(6), 1349-1359.
5. Chinthapalli, K. (2017). Ransomware attacks on healthcare: What you need to know. BMJ, 358, j3417.
6. Cohen, I. G., & Mello, M. M. (2018). Ethical challenges in the use of electronic health records: A systematic review of the literature. Health Affairs, 37(2), 195-200.
7. Gordon, L. A., Loeb, M. P., & Zhou, L. (2021). The impact of cyber risk on healthcare organizations: A survey. Journal of Health Care Finance, 47(1), 1-14.
8. Jones, A. B., Smith, R. D., & Kumar, S. (2024). Human error in cybersecurity: A review of causes and consequences in healthcare. Health Informatics Journal, 30(2), 103-112.
9. Kebaso, M. (2021). Cybersecurity awareness among healthcare workers in Kenyan public hospitals: A case study. International Journal of Cybersecurity and Privacy, 5(2), 122-135.
10. Kimani, A., Muthoni, L., & Ndegwa, P. (2023). Data security challenges in Kenya's public healthcare sector. Nairobi: African Cybersecurity Journal.
11. Kruse, C. S., Frederick, B., & Jacobson, T. (2017). Cybersecurity in healthcare: A systematic review of the literature. BMC Health Services Research, 17(1), 1-10.
12. Mbugua, M., Ndung'u, N., & Kiilu, J. (2021). Enhancing cybersecurity awareness in healthcare institutions: The role of training programs. International Journal of Information Systems and Project Management, 9(1), 31-44.
13. Miller, A. R., Moulton, J., & Dempsey, G. (2020). Assessing the state of cybersecurity in electronic health record systems: A survey of providers in LMICs. Journal of Health Information Management, 34(3), 105-113.
14. Ministry of Health. (2021). National eHealth policy 2021-2025: Enhancing healthcare through digitization. Nairobi, Kenya: Ministry of Health.
15. Muiruri, L., & Wanyoike, J. (2019). Security challenges of electronic health management systems in Kenyan public hospitals: A review. International Journal of Healthcare Management, 12(2), 71-79.
16. Muli, J. (2022). Cybersecurity in healthcare: Risks and recommendations for Kenyan hospitals. Journal of Health Informatics in Africa, 9(1), 34-45.
17. Oduor, J. & Wanyeki, B. (2021). Ransomware attacks on healthcare facilities in Kenya: Trends and implications. Kenya Journal of Cybersecurity, 2(1), 15-22.
18. Ouma, E. (2021). The state of data security in Kenya's healthcare sector: Current practices and future directions. International Journal of Information Security, 15(2), 78-88.
19. Raghavan, P., & Menon, V. (2022). The role of encryption in healthcare data security: Challenges and solutions. International Journal of Medical Informatics, 163, 104-115.
20. Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from health information technology–related adverse events. Journal of the American Medical Informatics Association, 23(6), 1076-1081.
21. Smith, T., & Chen, W. (2023). Backup and recovery strategies for ransomware attacks in healthcare: A systematic review. Journal of Information Systems Security, 19(3), 66-81.
22. Verma, A., & Raman, R. (2019). Cybersecurity in healthcare: Challenges and strategies for improvement. International Journal of Health Services, 49(4), 604-620.
23. Were, A., Namasasu, R., & Makori, J. (2020). Addressing cybersecurity in Kenyan public healthcare: Challenges and opportunities. International Journal of Cybersecurity and Privacy, 4(3), 99-115.
24. World Health Organization. (2022). Digital health in Africa: Advancements and challenges. Geneva: WHO.