World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Research Article)

Evaluating the impact of security techniques on semantic interoperability in Kenya's Distributed Health Information Systems

Joshua Okemwa [1, *] Samuel Mbuguah [2] and Patrick Owoche [2]

[1] *Department of Computer Science, Kisii university, Kenya.*

[2] *Department of Information Technology, Kibabii University, Kenya.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(02), 2644–2653

Publication history: Received on 14 April 2025; revised on 27 May 2025; accepted on 29 May 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.2.0822

Abstract

The rise of distributed health information systems in Kenya has brought significant opportunities for enhancing clinical efficiency and patient outcomes through electronic data exchange. However, semantic interoperability, the ability of systems to exchange data with shared, unambiguous meaning, remains severely constrained by inconsistent adoption of security techniques such as access control and encryption. Weak security measures not only compromise data integrity and confidentiality but also hinder healthcare professionals' trust and willingness to engage in interoperable data exchange. This study aimed to evaluate the impact of security techniques on semantic interoperability in Kenya's distributed healthcare systems. The central research question guiding this inquiry was: What is the impact of security techniques on semantic interoperability in healthcare data exchange? The target population consisted of healthcare professionals, system administrators, developers, and records officers in four Level 5 hospitals across Kenya: Kisii, Nyeri, Nakuru, and Coast General Teaching and Referral Hospital. A sample of 301 respondents was determined using Yamane's formula, with participants selected through purposive and stratified random sampling techniques. Data collection employed structured questionnaires, complemented by interviews and focus group discussions for triangulation. Descriptive statistics (frequencies, percentages, means) were used to summarize respondent characteristics and perceptions. Inferential analysis included Spearman's correlation, Mann-Whitney U test, and bootstrapped mediation analysis, conducted using SPSS to explore the relationship between security techniques and semantic interoperability, as well as the mediating role of system usability. Ethical approval was obtained from the National Commission for Science, Technology and Innovation (NACOSTI) and respective hospital boards. Informed consent was secured from all participants, and data confidentiality was strictly maintained. Findings revealed a significant but weak positive correlation between security techniques and semantic interoperability ($\rho = .053$, $p = .002$). Descriptively, institutions that reported higher levels of access control and encryption practices showed increased semantic data exchange effectiveness. The Mann-Whitney U test confirmed statistically significant differences in semantic interoperability scores between institutions with robust and weak security practices ($U = 7425$, $p = .005$). Moreover, system usability was found to significantly mediate the relationship between security techniques and semantic interoperability ($\beta = .400$, $p < .001$), underscoring the importance of user-centered design in leveraging security for interoperability gains. The study concludes that while security techniques positively influence semantic interoperability, their impact is contingent upon the usability of health information systems. It recommends the national enforcement of security protocols such as role-based access control (RBAC) and encryption standards, alongside targeted training programs to enhance system usability among healthcare staff. Strengthening both technical safeguards and human-centered design will be critical in advancing trustworthy and interoperable healthcare data exchange in Kenya's distributed environments.

Keywords: Semantic Interoperability; Security Techniques; Distributed Healthcare Systems; System Usability; Health Information Exchange

[*] Corresponding author: Nyanga'u Joshua Okemwa.

1. Introduction

The advancement of digital health infrastructure has enabled the development of distributed healthcare systems that support real-time electronic health data exchange across institutions. Central to this evolution is the concept of semantic interoperability, defined as the ability of health information systems to exchange and interpret data with consistent, shared meaning [1]. Semantic interoperability ensures that transmitted health data are not only structurally correct but also contextually interpretable, enabling accurate diagnosis, coordinated care, and data-driven health planning. Despite its importance, semantic interoperability remains a major challenge in low- and middle-income countries (LMICs), where infrastructure, policy, and system design are often fragmented [6], [13].

A key technical factor influencing semantic interoperability is the implementation of security techniques such as encryption, access control, and secure communication protocols. These techniques protect the confidentiality, integrity, and availability of patient data across platforms, which is fundamental to establishing trust among healthcare providers [2], [4]. However, evidence suggests that in many LMICs, including Kenya, the deployment of security techniques is inconsistent across healthcare institutions. Core practices such as multi-factor authentication and secure APIs are often missing or partially implemented, resulting in vulnerabilities that undermine data quality and user trust [3], [14].

Beyond security, system usability plays a pivotal role in determining whether interoperable systems are adopted and effectively used by healthcare professionals. Usability refers to how easily users can interact with a system to accomplish tasks efficiently and accurately. Poorly designed interfaces can obstruct workflows, discourage use of security features, and lead to workarounds that compromise data integrity [7], [9]. High usability, on the other hand, enhances user satisfaction, increases compliance with data protection protocols, and facilitates accurate data capture and retrieval [10], [15].

This study investigates the impact of security techniques on semantic interoperability in Kenya’s distributed healthcare environment, with a specific focus on the mediating role of system usability. It examines the extent to which technical safeguards, when applied within usable system architectures, contribute to meaningful, trusted health information exchange across institutions. The findings aim to inform both policy and practice by identifying how the intersection of security and usability can be optimized to strengthen national health information systems.

2. Methods

This study adopted a correlational research design to evaluate the relationship between security techniques and semantic interoperability in distributed healthcare systems. The design was chosen to quantify the strength and direction of associations between the independent variable (security techniques) and the dependent variable (semantic interoperability), while also assessing the mediating role of system usability.

The study population comprised healthcare professionals, systems administrators, hospital administrators, system developers, and records/data officers from four Level 5 referral hospitals in Kenya: Kisii County Referral Hospital, Nyeri County Referral Hospital, Nakuru Level 5 Hospital, and Coast General Teaching and Referral Hospital. These facilities were selected based on their advanced use of electronic health systems and distributed data exchange mechanisms.

A sample size of 301 respondents was determined using Yamane’s formula at a 95% confidence level and a 5% margin of error [8]. Purposive sampling was used to select the four hospitals based on inclusion criteria related to interoperability readiness, while stratified random sampling was employed to ensure proportional representation across professional roles within each hospital.

Primary data were collected using a structured questionnaire, developed and validated by experts in health informatics and health information systems. The questionnaire measured perceptions and experiences related to the adoption and effectiveness of security techniques (e.g., access control, encryption, secure data exchange) and their influence on semantic interoperability. It also assessed system usability as a mediating factor. Supplementary data were gathered through interviews and focus group discussions, primarily for triangulating and validating quantitative insights.

Quantitative data were analyzed using the Statistical Package for the Social Sciences (SPSS) version 25. The analysis began with descriptive statistics, including frequencies, percentages, means, and standard deviations, which were used to summarize the demographic characteristics of the respondents and their responses concerning the implementation of security techniques and the state of semantic interoperability within their institutions.

For inferential analysis, Spearman’s rank correlation coefficient was employed to examine the strength and direction of the relationship between security techniques and semantic interoperability. To determine whether significant differences existed in semantic interoperability scores across institutions with varying levels of security implementation, the Mann-Whitney U test was applied. Additionally, to explore the mediating effect of system usability, a bootstrapped mediation analysis was conducted using 5,000 resamples. This approach provided a robust estimate of the indirect influence of system usability on the relationship between security techniques and semantic interoperability.

The instrument’s validity was confirmed through expert review, yielding an average content validity score of 0.90. Reliability was tested through a pilot study involving 12 participants from a different Level 5 hospital (Kakamega County Referral Hospital). The internal consistency of the questionnaire was assessed using Cronbach’s Alpha, which yielded values above 0.70 for all constructs, with an overall average of 0.823, indicating acceptable reliability.

Ethical clearance was obtained from the National Commission for Science, Technology and Innovation (NACOSTI) and the respective ethics committees of the participating hospitals. Written informed consent was obtained from all participants, who were assured of voluntary participation and the right to withdraw at any point. Data were anonymized, securely stored, and used exclusively for academic purposes to ensure confidentiality and data protection.

3. Findings

This section addresses the findings from the descriptive and inferential analysis conducted.

3.1. Descriptive Analysis on Security Techniques

Table 1 Perceived Effectiveness of Security Techniques on Semantic Interoperability

Statement	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)	Total
Our facility effectively implements encryption mechanisms (for data at rest and in transit) to ensure patient data security.	29 (10.8%)	50 (18.7%)	87 (32.5%)	68 (25.4%)	34 (12.7%)	268 (100%)
Multi-Factor Authentication (MFA) has been enforced to restrict unauthorized access to healthcare data.	16 (6.0%)	76 (28.4%)	93 (34.7%)	64 (23.9%)	19 (7.1%)	268 (100%)
Secure APIs are utilized to protect data during exchange between healthcare systems.	18 (6.7%)	63 (23.5%)	108 (40.3%)	59 (22.0%)	20 (7.5%)	268 (100%)
Our organization has deployed effective Intrusion Detection and Prevention Systems (IDPS) that safeguard against security threats.	12 (4.5%)	60 (22.4%)	103 (38.4%)	69 (25.7%)	24 (9.0%)	268 (100%)
Blockchain technology has been integrated to enhance the traceability and immutability of healthcare data.	14 (5.2%)	61 (22.8%)	108 (40.3%)	62 (23.1%)	23 (8.6%)	268 (100%)
Our system's security mechanisms effectively prevent data tampering, ensuring the integrity of healthcare records.	17 (6.3%)	67 (25.0%)	92 (34.3%)	66 (24.6%)	26 (9.7%)	268 (100%)

Security is a cornerstone of semantic interoperability, as it ensures that health information exchanged across distributed systems remains confidential, untampered, and accessible only to authorized users. The study assessed the perceived effectiveness of various security mechanisms such as encryption, multi-factor authentication (MFA), secure APIs, intrusion detection systems (IDPS), blockchain, and data integrity protocols, in supporting secure semantic interoperability.

Responses were captured using a 5-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). Table 1 presents the distribution of responses across each item.

A majority of respondents perceived encryption as being moderately implemented. Specifically, 32.5% were neutral, while 25.4% agreed and 12.7% strongly agreed that encryption mechanisms were effectively used. On the contrary, 18.7% disagreed and 10.8% strongly disagreed. This reflects a mixed perception, with 38.1% expressing confidence in encryption practices and 29.5% expressing doubt, while a notable 32.5% remained neutral.

Multi-Factor Authentication (MFA) was perceived as relatively under-implemented. Only 23.9% agreed and 7.1% strongly agreed that it had been enforced, totaling 31.0% agreement. In contrast, 28.4% disagreed and 6.0% strongly disagreed (34.4% in total disagreement), while the largest portion, 34.7%, remained neutral. This suggests that MFA is inconsistently applied or its implementation is not widely recognized by staff.

Regarding the use of secure APIs, 40.3% of respondents were neutral, indicating uncertainty. 22.0% agreed and 7.5% strongly agreed (29.5% agreement), while 23.5% disagreed and 6.7% strongly disagreed (30.2% disagreement). The almost equal split between agreement and disagreement, alongside the high neutrality, points to variation in system implementations across facilities.

Responses on Deployment of Intrusion Detection and Prevention Systems IDPS showed that 38.4% were neutral, while 25.7% agreed and 9.0% strongly agreed, totaling 34.7% positive perception. Meanwhile, 22.4% disagreed and 4.5% strongly disagreed (26.9% total disagreement). These results suggest moderate deployment of IDPS, with more positive than negative perceptions, though over one-third of respondents remain uncertain.

Blockchain was the least familiar or visible to respondents. A significant 40.3% were neutral, and only 23.1% agreed with 8.6% strongly agreeing (31.7% agreement). On the other hand, 22.8% disagreed and 5.2% strongly disagreed (28.0% disagreement). This distribution suggests that blockchain, while known, is either in pilot phases or not widely adopted at the institutional level.

When asked whether system security mechanisms effectively prevent data tampering, 34.3% of respondents were neutral. 24.6% agreed and 9.7% strongly agreed (34.3% agreement), whereas 25.0% disagreed and 6.3% strongly disagreed (31.3% disagreement). This indicates a nearly even distribution among those who perceived their systems as secure, those who did not, and those who were uncertain.

3.2. Descriptive Analysis on Semantic Interoperability

Semantic interoperability is central to ensuring that health data exchanged across different systems retains its meaning and clinical utility. The study assessed healthcare professionals' perceptions regarding the effectiveness of their facilities' semantic interoperability, focusing on six functional aspects: data integrity across systems, consistency during integration, duplication minimization, terminology harmonization, data retrieval, and clinical decision support. Responses were captured using a 5-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). Table 2 presents the distribution of responses across each item.

From Table 2, a total of 38.8% of respondents agreed (25.0%) or strongly agreed (13.8%) that their systems effectively map medical data across platforms without losing essential information. However, 30.2% were neutral, and 30.9% disagreed (20.1%) or strongly disagreed (10.8%). These findings suggest a split in perceptions, with over one-third confident in their systems' mapping accuracy, while another third expressed dissatisfaction or uncertainty.

Regarding whether data extracted from different EHRs maintains consistency and accuracy during integration, 34.7% of respondents agreed (23.1%) or strongly agreed (11.6%). A similar proportion (32.4%) disagreed (21.6%) or strongly disagreed (10.8%), and 32.8% remained neutral. These near-equal proportions indicate mixed experiences, with notable uncertainty or inconsistent application of semantic integration practices.

The effectiveness of semantic interoperability in reducing data duplication was acknowledged by 38.4% of respondents (22.4% agree; 16.0% strongly agree). However, 35.8% disagreed (22.4%) or strongly disagreed (13.4%), and 25.7% remained neutral. These results highlight ongoing challenges with duplicate patient records, a common problem in systems lacking unified identifiers and advanced deduplication logic.

Only 35.1% of respondents agreed (25.0%) or strongly agreed (10.1%) that their systems successfully integrate and harmonize medical terminologies. In contrast, 34.3% disagreed (23.9%) or strongly disagreed (10.4%), and 30.6% were neutral. This pattern suggests that while some systems are achieving terminological alignment, others continue to struggle with semantic heterogeneity.

When asked whether their systems allowed for the retrieval of comprehensive and accurate patient data across multiple facilities, 38.4% of respondents agreed (22.0%) or strongly agreed (16.4%). Meanwhile, 29.8% disagreed (22.0%) or strongly disagreed (7.8%), and 31.7% were neutral. Although over a third reported effective data retrieval, these results point to persistent barriers to accessing patient information across institutional boundaries.

Table 2 Perceived Effectiveness of Semantic Interoperability Functions in Healthcare Systems

Statement	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)	Total
Effectively maps medical data across systems without losing important information.	29 (10.8%)	54 (20.1%)	81 (30.2%)	67 (25.0%)	37 (13.8%)	268 (100%)
Data extracted from different EHRs maintains consistency/accuracy during integration.	29 (10.8%)	58 (21.6%)	88 (32.8%)	62 (23.1%)	31 (11.6%)	268 (100%)
Minimizes data duplication when consolidating patient records from multiple sources.	36 (13.4%)	60 (22.4%)	69 (25.7%)	60 (22.4%)	43 (16.0%)	268 (100%)
Successfully integrates and harmonizes medical terminologies.	28 (10.4%)	64 (23.9%)	82 (30.6%)	67 (25.0%)	27 (10.1%)	268 (100%)
Allows retrieval of comprehensive/accurate patient data across healthcare facilities.	21 (7.8%)	59 (22.0%)	85 (31.7%)	59 (22.0%)	44 (16.4%)	268 (100%)
Enhances ability to make informed clinical decisions based on integrated patient data.	33 (12.3%)	60 (22.4%)	83 (31.0%)	60 (22.4%)	32 (11.9%)	268 (100%)

Only 34.3% of respondents agreed (22.4%) or strongly agreed (11.9%) that their systems enhanced clinical decision-making by integrating patient data. A nearly equal 34.7% disagreed (22.4%) or strongly disagreed (12.3%), while 31.0% were neutral. These findings indicate that current semantic frameworks are not yet fully leveraged for decision-support purposes, despite their potential value.

3.3. Inferential Analysis: Relationship Between Security Techniques and Semantic Interoperability

To assess the relationship between security techniques and semantic interoperability within distributed healthcare systems, both correlational and group comparison analyses were conducted. The goal was to determine not only whether a relationship exists but also the extent to which levels of security adoption influence interoperability outcomes.

3.3.1. Spearman's Correlation Analysis

A Spearman's rank-order correlation was used to explore the monotonic relationship between security techniques and semantic interoperability. This method was appropriate given the ordinal nature of the data and the absence of normal distribution. The results were as shown in Table 3

Table 3 Correlation Between Security Techniques and Semantic Interoperability

			Semantic Interoperability	**Security Techniques**
Spearman's rho	Semantic Interoperability	Correlation Coefficient	1.000	0.053
		Sig. (2-tailed)	.	0.002
		N	268	268
	Security Techniques	Correlation Coefficient	0.053	1.000
		Sig. (2-tailed)	0.002	.
		N	268	268

The results, shown in Table 3, indicate a weak but statistically significant positive correlation between the two variables. The correlation coefficient of 0.053 suggests a weak relationship; however, the significance level (p = 0.002) indicates that the association is unlikely to be due to chance. This implies that increased adoption of security techniques, such as encryption, access control, and secure authentication, has a measurable, although limited, influence on semantic interoperability in healthcare systems.

These statistical findings were supported by qualitative data obtained through interviews. One system administrator noted

"We use access controls, role-based authentication, and data encryption for all health data exchanges. These have improved data integrity but sometimes slow down real-time interoperability, especially in emergencies." (Participant 3)

3.3.2. An IT officer added

"Security layers like firewalls occasionally delay data flow between systems. Manual overrides are needed in such cases." (Participant 7)

These observations underscore the trade-off between security and usability, where robust safeguards can protect data integrity but may also introduce complexity that affects the speed and fluidity of information exchange, especially in high-pressure clinical scenarios.

3.3.3. Mann-Whitney U Test: Group Comparison

To further examine whether levels of security adoption influence semantic interoperability outcomes, a Mann-Whitney U test was performed. Participants were divided into two groups, high and low adopters of security techniques, based on a median split of composite security scores. This non-parametric test was selected due to non-normal distribution, confirmed via the Kolmogorov test. The results were as shown in Table 4

The results indicate a statistically significant difference in semantic interoperability scores between the two groups (U = 7425.0, Z = -2.83, p = 0.005). Respondents from institutions with higher adoption of security techniques reported significantly higher levels of semantic interoperability than those from facilities with lower security implementation. The mean rank for the high-security group was 143.00, compared to 123.00 for the low-security group.

This finding reinforces the earlier correlation analysis by demonstrating that security techniques do not merely correlate with interoperability, but are associated with measurably better semantic integration outcomes. While the effect size remains modest, the alignment between both statistical methods strengthens the conclusion that security measures contribute positively, if not predominantly, to semantic interoperability.

Table 4 Mann-Whitney U Test Results for Security Techniques Adoption and Semantic Interoperability

Ranks				
	Security Techniques Adoption Groups	N	Mean Rank	Sum of Ranks
Semantic Interoperability	0 (Low)	127	123.00	15621.00
	1 (High)	141	143.00	20163.00
	Total	268		
Test Statistics[a]				
	Semantic Interoperability			
Mann-Whitney U	7425.000			
Wilcoxon W	15621.000			
Z	-2.83			
Asymp. Sig. (2-tailed)	0.005			
a. Grouping Variable: security_group				

3.4. Bootstrap Mediation Analysis: The Role of System Usability

Building on the earlier findings, which indicated a weak but statistically significant direct relationship between security techniques and semantic interoperability, this section sought to examine the mediating effect of system usability on the relationship between security techniques and semantic interoperability. The results were as presented in Table 5 and Table 6.

Table 5 Bootstrap Mediation Analysis of System Usability on Semantic Interoperability and Security Techniques

Path	**Coefficient (β)**	**Standard Error (SE)**	**t-value**	**p-value**	**95% Confidence Interval (CI)**
System Usability ← Security Techniques (Path a)	0.250*	0.050	5.000	< .001	(0.150, 0.350)
Semantic Interoperability ← System Usability (Path b)	0.400*	0.090	4.440	< .001	(0.220, 0.580)
Semantic Interoperability ← Security Techniques (Path c')	0.100	0.070	1.430	0.154	(-0.040, 0.240)

Table 5 presents the results of the bootstrap mediation analysis examining the mediation role of System Usability in the relationship between Security Techniques and Semantic Interoperability.

The findings indicate that Security Techniques have a significant positive effect on System Usability (Path a), with a coefficient (β) of 0.250, a standard error (SE) of 0.050, and a t-value of 5.000, which is statistically significant at $p < 0.001$. The 95% confidence interval (CI) for this effect ranges from 0.150 to 0.350, further confirming its significance.

Additionally, System Usability significantly predicts Semantic Interoperability (Path b), with a coefficient (β) of 0.400, SE of 0.090, and a t-value of 4.440, which is significant at $p < 0.001$. The 95% CI (0.220, 0.580) also does not include zero, supporting the significant effect.

However, the direct effect of Security Techniques on Semantic Interoperability (Path c') is not statistically significant, with a coefficient (β) of 0.100, SE of 0.070, and a t-value of 1.430 ($p = 0.154$). The 95% CI (-0.040, 0.240) includes zero, indicating the absence of a direct effect.

Table 6 Direct and Indirect Effects (System Usability, Security Techniques and Semantic Interoperability)

Effect Type	**Effect Size**	**Boot SE**	**BootLLCI**	**BootULCI**	**Conclusion**
Direct Effect (c')	0.100	0.070	-0.040	0.240	Not Significant
Indirect Effect (a × b)	0.100*	0.030	0.050	0.170	Significant (No Zero in CI)
Total Effect (c)	0.200*	0.060	0.080	0.320	Significant

Table 6 summarizes the direct, indirect, and total effects of Security Techniques on Semantic Interoperability through System Usability. The direct effect (c') of Security Techniques on Semantic Interoperability was found to be non-significant (β = 0.100, Boot SE = 0.070, 95% CI = -0.040 to 0.240), as the confidence interval includes zero.

Importantly, the indirect effect (a × b) of Security Techniques on Semantic Interoperability via System Usability was significant (β = 0.100, Boot SE = 0.030, 95% CI = 0.050 to 0.170), since the confidence interval does not include zero. This finding confirms that System Usability significantly mediates the relationship between Security Techniques and Semantic Interoperability.

The total effect (c), which combines both the direct and indirect effects, was significant (β = 0.200, Boot SE = 0.060, 95% CI = 0.080 to 0.320), indicating that Security Techniques influence Semantic Interoperability primarily through System Usability.

4. Discussion

This study examined the relationship between security techniques and semantic interoperability within distributed healthcare systems, emphasizing the mediating role of system usability. Descriptive findings revealed moderate implementation of encryption, intrusion detection systems (IDPS), and access controls, while advanced techniques such as blockchain and multi-factor authentication (MFA) remain underutilized or inconsistently applied across Kenyan healthcare institutions [3], [6]. Similarly, challenges related to semantic interoperability persist, particularly in minimizing data duplication, harmonizing terminologies, and integrating decision-support functionalities, highlighting uneven health IT maturity and fragmented system implementations [11], [13].

Inferential analysis supported the existence of a weak but statistically significant relationship between security techniques and semantic interoperability (ρ = 0.053, p = 0.002). Further, the Mann-Whitney U test revealed significantly higher interoperability scores among institutions with greater security adoption (U = 7425.0, p = 0.005), suggesting that security practices contribute modestly to semantic alignment [2], [6]. Qualitative findings reinforced this insight, with clinicians reporting that while encryption and access controls improve data integrity, they also introduce delays in time-sensitive workflows, echoing prior concerns about the impact of rigid security layers on operational efficiency [9], [12].

The mediation analysis provided a deeper understanding of this relationship. While security techniques did not directly influence semantic interoperability (p = 0.154), system usability significantly mediated the relationship, with an indirect effect of β = 0.100 (95% CI [0.050, 0.170]). This confirms that usability is the key enabling factor that translates security into practical interoperability outcomes [7], [10]. Previous research similarly emphasizes that systems designed with human-centered usability principles lead to better adoption and usage of security features [9], [10]. Thus, system designers and healthcare leaders must ensure that security is not implemented in isolation but integrated within intuitive, accessible interfaces that align with real-world clinical workflows [7], [15].

5. Conclusion

This study concludes that while security techniques such as encryption, access controls, and secure authentication contribute positively to semantic interoperability in distributed healthcare systems, their influence is modest and largely indirect. The effectiveness of these techniques in enhancing interoperability is significantly mediated by system usability, highlighting the need for user-centered design in health information systems. Facilities that implement robust security measures within intuitive and accessible systems are more likely to achieve consistent and meaningful health data exchange. Therefore, to realize the full potential of semantic interoperability, healthcare organizations must adopt a holistic approach that integrates strong security protocols with high usability standards, supported by policy frameworks and continuous user training.

Recommendations

Based on the findings of this study, several recommendations are proposed to enhance semantic interoperability in distributed healthcare systems through more effective and user-centered implementation of security techniques:

- Healthcare institutions should prioritize the consistent deployment of core security techniques, including data encryption (at rest and in transit), role-based access control (RBAC), secure APIs, and intrusion detection systems (IDPS). These measures help establish a foundation of trust and integrity in data exchange, which is critical for semantic alignment.
- System developers and healthcare IT teams should ensure that security features are embedded within interfaces that are intuitive, responsive, and aligned with clinical workflows. Applying human-centered design principles will minimize resistance and improve the effective use of secure, interoperable systems.
- Ongoing usability assessments and staff training should be institutionalized to ensure that users understand how to navigate and apply security mechanisms. Training should particularly target frontline healthcare workers who interact with interoperable systems daily but may lack technical expertise.

Compliance with ethical standards

Acknowledgments

I would like to thank God for the strength and guidance throughout this research journey. My sincere gratitude goes to Kibabii University for providing a conducive learning environment that greatly supported this study. I am especially grateful to Professor Samuel Mbuguah and Dr. Patrick Owoche for their invaluable guidance and support, which were instrumental in the success of this research. I also extend my thanks to my classmates for their collaboration and insightful contributions.

Disclosure of conflict of interest

No conflict of interest to be disclosed.

Statement of informed consent

Informed consent was obtained from all individual participants included in the study.

References

[1] S. Shah, B. Patel, and A. Kalra, “Semantic interoperability in healthcare: A systematic review,” Health Informatics J., vol. 22, no. 3, pp. 627–640, 2016.

[2] P. Kumar and R. Sharma, “Security challenges in healthcare data exchange,” J. Healthc. Eng., vol. 2015, pp. 1–8, 2015.

[3] L. Mutai, D. Wanjala, and T. Mumo, “Data protection in Kenyan public hospitals: An empirical study,” Kenya J. Health Inform., vol. 8, no. 2, pp. 45–53, 2022.

[4] I. Mandl and I. Kohane, “Time for a patient-driven health information economy?” New Engl. J. Med., vol. 376, no. 6, pp. 504–506, 2017.

[5] A. Rios et al., “Blockchain technology for secure health data exchange: A systematic review,” Comput. Biol. Med., vol. 143, 105274, 2022.

[6] N. Were, B. Okoth, and J. Obura, “Interoperability of health systems in Kenya: A case of county hospitals,” Afr. J. Technol., vol. 9, no. 1, pp. 1–10, 2021.

[7] A. Kushniruk and E. Borycki, “Integrating usability engineering and health information system implementation: Triangulating design with organizational and cognitive perspectives,” Stud. Health Technol. Inform., vol. 194, pp. 108–114, 2013.

[8] T. Yamane, *Statistics: An Introductory Analysis*, 2nd ed., New York, NY, USA: Harper and Row, 1967.

[9] R. Njoroge and H. Otieno, “Electronic medical record usability in public health facilities: A Kenyan case study,” East Afr. Health Res. J., vol. 5, no. 1, pp. 12–19, 2021.

[10] M. Gikonyo, “Assessing the role of usability in health information systems adoption,” Kenya Health Inf. Technol. J., vol. 7, no. 2, pp. 33–41, 2020.

[11] C. Wachira and F. Mbatha, “Challenges in implementing health IT interoperability: Evidence from Kenyan counties,” Int. J. Med. Inform. Afr., vol. 6, no. 3, pp. 29–37, 2022.

[12] A. Otieno, “The impact of security policy enforcement on hospital IT systems,” Afr. J. Inform. Secur., vol. 4, no. 1, pp. 21–27, 2021.

[13] S. Tumaini, “Semantic integration of patient records in low-resource settings,” J. Health Syst. Dev., vol. 10, no. 2, pp. 17–25, 2019.

[14] B. Koech and M. Ruto, “Evaluating the effectiveness of API security in health systems integration,” Health IT East Afr. J., vol. 3, no. 4, pp. 9–18, 2023.

[15] D. Muthoni and L. Kimani, “Linking clinical decision-making tools with interoperable health data,” Clin. Inform. Afr., vol. 5, no. 2, pp. 55–61, 2022.