IOSR Journal Of Humanities and Social Science (IOSR-JHSS)
Volume 30, Issue 10, Series 1 (October, 2025) 44-48
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Legal Challenges Of Implementing Information Security Metrics For Patient Safety In Kenyan Public Hospitals: An Empirical Review Under The Data Protection Act, 2019

Maryanne Waithera Mwaura, Dr. Bernard Munyao Muiya
Kenyatta University, Kenya

Abstract
Background: *As the healthcare sector embraces digital transformation, the use of Information Security Metrics (ISM) has become central to protecting patient data and improving patient safety. However, the effectiveness of ISM is constrained by legal and institutional challenges, especially in public health systems. This study analyses the legal challenges associated with using ISM to enhance patient safety in public hospitals within Nairobi Metropolitan, with reference to the Kenyan Data Protection Act, No. 24 of 2019.*
Materials and Methods*: Using a quantitative design, the study collected data from health professionals involved in data governance and patient care. Descriptive statistics and exploratory factor analysis revealed strong institutional awareness of legal obligations but identified weaknesses in patient engagement and consent practices. While formal data protection policies and legal implications for data breaches were widely acknowledged, neutral responses around patient inclusion highlight disconnect between regulatory compliance and patient-centred implementation.*
Results: *Kenyan public hospitals have moderate legal and policy frameworks for data governance, with an overall mean score of 3.52. Most staff acknowledged the existence of legal mechanisms such as the Data Protection Act and Health Act, but their actual enforcement and patient engagement practices were inconsistent. Exploratory factor analysis showed a strong single factor Legal Compliance and Data Governance explaining 78% of variance, but operational gaps remain, particularly in consent tracking and breach reporting. The results highlight that legal compliance is more formal than practical, with limited staff capacity to implement information security metrics. Strengthening enforcement, capacity building, and patient involvement is essential for effective data protection.*
Conclusion: *The findings underscore the need for institutional reforms that integrate legal frameworks with participatory data governance. There is need for structured consent mechanisms, staff training on the Data Protection Act, and enhanced oversight to ensure that legal compliance translates into improved patient safety.*
Keywords: *Information Security Metrics, Patient Safety, Data Protection Act, Legal Challenges, Public Hospitals, Health Information Governance, Kenya*

Date of Submission: 25-09-2025 Date of Acceptance: 05-10-2025

I. Introduction

The global shift toward digitized healthcare has elevated the importance of Information Security Metrics (ISM) quantitative indicators used to measure the effectiveness of security controls. ISM support patient safety by monitoring compliance, preventing unauthorized access, and ensuring data confidentiality, integrity, and availability.[1] In advanced healthcare systems such as those in the United States and Europe, ISM supports regulatory compliance and clinical decision-making by providing performance dashboards aligned with legal standards like HIPAA in the US and GDPR in the EU.

In the United States, the rise in hospital cyberattacks particularly ransomware events has catalysed enhanced legal scrutiny of data safety. A Senate bill proposed in late 2024 mandates multifactor authentication, regular security audits, and stricter HIPAA compliance enforcement for providers in 2025.[2] However, human error remains a significant security threat: a study of data breaches from 2009 to 2023 found that most incidents in US healthcare systems were triggered by human behaviour, despite existing HIPAA mandates.[3] Importantly, US research has shown that data breaches correlate with measurable declines in patient care quality such as increased 30-day mortality rates following myocardial infarction highlighting the link between legal compliance, data security, and clinical outcomes.[4]

In Asia, the SingHealth cyberattack in Singapore exposed systemic vulnerabilities in staff training, incident response, and governance despite advanced technical infrastructure.[5] The subsequent independent inquiry recommended extensive security governance reforms, regular staff training, and enhanced audit protocols to align legal compliance with operational practice.[7] Sub-Saharan Africa, including South Africa, Ghana, Uganda, and Nigeria, has seen recent enactment of data protection legislation often modelled on GDPR but institutionalization remains a challenge.[8] A comparative study highlighted that while these countries provide lawful data processing frameworks, actual implementation in healthcare systems is hindered by limited resources and weak enforcement.[9]

In Kenya, rapid digital transformation including rollout of e-health platforms, mobile health (m-health) apps, and telemedicine has created urgent needs for robust data governance.[10] The Data Protection Act, No. 24 of 2019 established strong statutory obligations including data subject rights, breach notification, privacy by design, and mandatory appointment of Data Protection Officers.[11] The Act designates health data as sensitive personal data, making it subject to heightened legal safeguards.[12]

Despite this progressive legal architecture, public hospitals face multiple legal challenges in using ISM to enhance patient safety.[13] These include weak consent protocols, fragmented information systems, inconsistent legal awareness among staff, and a lack of integration between legal metrics (e.g., audit trails of consent, breach reporting) and technical ISM dashboards.[14, 15] A detailed Kenyan brief on the further emphasizes data governance challenges including interoperability, integrated patient records, and accountability mechanisms.[16] Kenya's journey toward unified e-health governance through initiatives like KeHMIS and its interoperability layer demonstrates high potential for system-wide metrics.[17] Yet operationalizing the Act's consent requirements and legal safeguards remains uneven (Health Data Governance, Kenya case study). In practice, ISM dashboards in many hospitals emphasize technical indicators, while legal dimensions such as patient consent, data subject rights, and breach accountability remain underrepresented despite their foundational role in achieving true patient safety.[18]

Viewed through Information Governance Theory, effective Information Security Metrics (ISM) should embed policy, culture, and accountability within institutional frameworks. However, public hospitals in Kenya often demonstrate disconnect between de jure compliance (formal policies) and de facto implementation (practical application).[19] In parallel, Regulatory Compliance Theory underscores how institutional readiness, staff awareness, and behavioural dynamics influence the extent to which legal obligations are internalized. While hospitals may formally adhere to the Data Protection Act, No. 24 of 2019, the absence of operational tools such as consent tracking systems, patient awareness protocols, and legal audit trails can significantly undermine the effectiveness of ISM in promoting patient safety.[20]

In light of these contextual and institutional dynamics, this paper investigates the legal challenges of using Information Security Metrics to enhance patient safety in public hospitals in Kenya. Drawing on the Kenyan Data Protection Act, No. 24 of 2019, the study explores how gaps in legal compliance, informed consent, and organizational data governance influence the implementation of ISM.[21] The findings are based on an empirical assessment conducted across public hospitals within Nairobi Metropolitan County.

The study draws on two theoretical foundations: Information Governance Theory and Regulatory Compliance Theory. Information Governance Theory posits that structured oversight of information through policies, roles, and accountability mechanisms is vital for organizational efficiency and compliance. In healthcare, this theory supports the structured use of ISM to manage patient data ethically and securely.

Regulatory Compliance Theory, on the other hand, emphasizes how institutions respond to external legal requirements. According to this theory, effective compliance requires not just formal adherence to laws, but also internal alignment in terms of culture, training, systems, and enforcement.[22] The Kenyan Data Protection Act thus becomes a compliance benchmark against which public hospitals' ISM practices can be evaluated.

II. Material And Methods

Study Design: This study employed a cross-sectional survey design to assess perceptions of legal compliance, data privacy, and governance practices in public referral hospitals within the Nairobi Metropolitan region. The cross-sectional design was appropriate for capturing respondent perceptions at a single point in time.[23]

Study Location: The study was carried out in public referral hospitals within the Nairobi Metropolitan region.

Sample Size: 288 respondents.

Sample size calculation: The study targeted key personnel involved in data management, including ICT officers, health records officers, nurses, and medical officers. A combination of stratified and purposive sampling was used to ensure representation across professional groups. Stratification was based on professional role, with proportional allocation according to the size of each group within the selected hospitals. Purposive sampling ensured that participants had direct experience with patient data management and legal compliance procedures. Sample size was determined using Slovin's formula, to provide adequate representation for Exploratory Factor Analysis (EFA) and descriptive analyses.

Subjects & selection method: Hospitals were purposively selected based on their size, level of digitization, and exposure to regulatory requirements, ensuring that participants had sufficient experience with electronic data management and compliance practices. Data collection was conducted over a two-month period. Ethical approval was obtained from the KNH-UON ERC, and written informed consent was secured from all participants prior to data collection. Participant confidentiality and anonymity were strictly maintained throughout the study.

Procedure methodology: Data were collected using a structured questionnaire designed around key constructs from the Data Protection Act, including legal compliance, patient data privacy, consent practices, and organizational data governance. The questionnaire used a 5-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree) to measure perceptions. Items were developed based on a review of relevant literature and legal frameworks and were reviewed by experts in health informatics and data governance to ensure content validity. The questionnaire was pilot-tested on 10% of the sample size (n = 29) to assess clarity, reliability, and feasibility. Minor adjustments were made based on pilot feedback to improve comprehensibility and item wording. Participants were given the option to complete the survey electronically or via paper forms, depending on accessibility.

Statistical analysis: Data were analysed using SPSS Version 26. Descriptive statistics (means, standard deviations, frequencies, and percentages) summarized respondents' perceptions of legal compliance and data governance practices. Exploratory Factor Analysis (EFA) using Principal Axis Factoring with Varimax rotation was conducted to identify latent legal constructs influencing Information Systems Management (ISM) effectiveness. Factor retention was based on eigenvalues greater than 1, inspection of the scree plot, and theoretical interpretability of factors. Items with factor loadings below 0.4 or cross-loadings on multiple factors were removed. Cronbach's alpha assessed internal consistency ($\alpha > 0.7$ considered acceptable). Missing data were minimal and handled using listwise deletion to maintain consistency in EFA. Results from EFA were used to inform subsequent analyses and interpretation of how legal and governance factors shape ISM effectiveness in hospital settings.

III. Result

Respondents generally agreed on the presence of legal mechanisms to support data governance in hospitals, though levels of engagement varied:

Table 1: Presence of Legal Mechanisms

Legal Compliance Item	Mean	Std. Dev.
Patient engagement and approval is granted beforehand	3.27	0.98
Patients are actively engaged in data collection	3.38	0.95
Patient data privacy and confidentiality is prioritized	3.70	1.03
Policies exist to protect confidentiality, integrity, and availability of data	3.67	1.00
Legal implications exist for unauthorized sharing or alteration of patient data	3.59	1.06

The overall mean score across items was 3.52, indicating moderate agreement with the existence of legal protections in data handling. However, the neutral ratings on patient engagement suggest operational inconsistencies.

Exploratory Factor Analysis (EFA)

To reduce dimensionality and uncover latent structures, EFA was performed using Principal Axis Factoring and Varimax rotation.

Table 2: Exploratory Factor Analysis

Variable Description	Extracted
Patient consent granted beforehand	0.633
Patients actively engaged in data collection	0.655
Patient data privacy prioritized	0.872
Policies to protect CIA of patient data	0.841

Variable Description	Extracted
Legal implications for unauthorized sharing or alteration of data	0.897

All items exceeded the 0.6 threshold, indicating they contributed strongly to the extracted factor.

Table 3: Total Variance Explained

Component	Initial Eigenvalue	% of Variance	Cumulative %
1	3.899	77.981%	77.981%

A single dominant factor explained nearly 78% of total variance, suggesting a coherent underlying construct labelled Legal Compliance and Data Governance.

Table 4: Rotated Component Matrix

Item Description	Factor Loading
Legal implications for unauthorized data handling	0.947
Data privacy and confidentiality prioritization	0.934
Formal data protection policies	0.917
Patient consent granted beforehand	0.796
Active patient engagement in data collection	0.809

IV. Discussion

This study sought to evaluate the legal and institutional dimensions shaping the implementation of information security metrics (ISM) to promote patient safety in public hospitals in Kenya. The findings revealed a moderate level of consensus among hospital staff regarding the extent to which legal and policy instruments particularly the Health Act and the Data Protection Act have been implemented at the operational level.

While respondents generally acknowledged the presence of regulatory frameworks, they expressed uncertainty and inconsistency in their actual enforcement across different departments. This aligns with the study's first major finding: that legal compliance exists more in principle than in practice. This distinction echoes observations by[5] in South Africa and in Ghana, who also noted that policy compliance does not necessarily translate to systemic behavioural change or effective implementation.[24]

Moreover, the findings suggest that staff capacity to apply security metrics such as those involving consent protocols and breach detection remains limited. This reinforces regulatory compliance theory, which posits that institutions may adopt formal policies without developing internal culture and capacity for actual implementation. Similar implementation gaps were observed in India and Singapore, where public institutions showed compliance on paper but struggled with real-time enforcement, especially in data governance practices.

A significant insight from this study is the legal blind spot concerning patient involvement. Although the Data Protection Act provides for patient agency in the handling of personal data, most respondents were unaware of mechanisms for consent tracking or complaints handling. This disconnect reveals a limitation in the application of Information Governance Theory in Kenya's health sector particularly its emphasis on accountability and transparency as pillars of data governance.

In comparing these findings to existing literature in Kenya, it becomes evident that the study builds on and deepens observations from the KeHMIS and CIPESA reports. While those studies focused on data availability and interoperability, this study highlights the legal and human dimensions particularly the structural barriers to integrating ISM into routine hospital operations.

The findings therefore extend existing knowledge by spotlighting the operational disconnect between regulatory intent and implementation practice. This adds nuance to Information Governance Theory by showing how policy frameworks, though essential, require embedded practices and institutional culture change to support patient safety effectively.

However, the study is not without limitations. Its scope was limited to select public hospitals, and the data were primarily self-reported, introducing potential bias. Further research is recommended to assess implementation in private health facilities and to examine patient awareness and experiences concerning data protection measures.

In sum, this study reinforces the need for not just regulatory frameworks but active, well-resourced institutional mechanisms that embed information security in day-to-day hospital practice. Future policies should prioritize capacity-building, accountability systems, and patient engagement as part of an integrated approach to ISM in Kenya's healthcare system.

V. Conclusion

Hospitals should adopt digital consent systems, train staff on the Data Protection Act, and raise patient awareness of data rights. Regular compliance audits and integrating patient safety with legal indicators will strengthen accountability and protect patient information effectively.

References

[1]. Abouelmehdi, K., Beni-Hssane, A., & Khaloufi, H. (2018). Big Data Security And Privacy In Healthcare: A Review. Procedia Computer Science, 113, 73–80. Https://Doi.Org/10.1016/J.Procs.2017.08.292

[2]. Choi, S. J., & Johnson, M. E. (2019). Do Hospital Data Breaches Reduce Patient Care Quality? Arxiv. Https://Doi.Org/10.1102/1904.02058

[3]. CIPESA. (2024, May 3). Kenya's Digital Health Act Protective Of Patients' Privacy Rights. CIPESA. Retrieved From Ifex.Org

[4]. Health Data Governance. (N.D.). Kenya: The Principles In Action. Health Data Governance. Retrieved From Healthdatagovernance.Org

[5]. Irene Tham & Hariz Baharudin. (2019). COI On Singhealth Cyber-Attack: 5 Key Findings. The Straits Times.

[6]. Kamande, K. (2024, December 22). Protection Of Patients' Data Vital. The Star. Retrieved From The-Star.Co.Ke

[7]. Moncy, M. M., Afreen, S., & Purkayastha, S. (2023). Healthcare Security Breaches In The United States: Insights And Their Socio-Technical Implications. Arxiv. Https://Doi.Org/10.1102/2311.03664

[8]. PMC. (2024). The Regulation Of Health Data Sharing In Africa: A Comparative Study. PMC. Retrieved From Pmc.Ncbi.Nlm.Nih.Gov

[9]. Reel Informatics. (2023). Kenyan Healthcare Data Security: Practical Lessons And Best Practices For Patient Privacy. Reel Informatics. Retrieved From Reelinformatics.Com

[10]. Rundle, J. (2024, December 27). Healthcare Providers Face Stiffer Cyber Rules Even As They Cry For Help. The Wall Street Journal.

[11]. Sentinel Africa. (2023). Ensuring Data Protection In The Health Sector. Sentinel Africa Consulting Ltd. Retrieved From Sentinelafricaconsulting.Com

[12]. Singhealth Breach Committee Of Inquiry. (2019). Recommendations To Boost Cybersecurity In Singapore Healthcare Sector. The Straits Times.

[13]. Tripleoklaw TMT Team. (2024). Ethical Issues On Health Technologies In The Wake Of The Data Protection Act. Tripleoklaw LLP. Retrieved From Tripleoklaw.Com

[14]. Abouelmehdi, K., Beni-Hssane, A., & Khaloufi, H. (2018). Big Data Security And Privacy In Healthcare: A Review. Procedia Computer Science, 113, 73–80. Https://Doi.Org/10.1016/J.Procs.2017.08.292

[15]. Amponsah, D. O. (2021). The Impact Of Information Security Practices On Patient Safety: A Ghanaian Case. Health Information Management Journal, 50(2), 107–115. Https://Doi.Org/10.1177/1833358320906822

[16]. Atkins, D., Kilbourne, A. M., & Shulkin, D. (2017). Moving From Discovery To System-Wide Change: The Role Of Research In A Learning Health Care System. Health Affairs, 36(4), 573–579. Https://Doi.Org/10.1377/Hlthaff.2016.1137

[17]. Chigada, J., & Madzinga, R. (2021). Information Security Governance In Healthcare: A South African Public Hospital Perspective. SA Journal Of Information Management, 23(1), 1–7. Https://Doi.Org/10.4102/Sajim.V23i1.1300

[18]. Government Of Kenya. (2019). Data Protection Act, No. 24 Of 2019. Nairobi: Government Printer. Https://Www.Odpc.Go.Ke

[19]. Hogan, W. R., & Wagner, M. M. (1997). Accuracy Of Data In Computer-Based Patient Records. Journal Of The American Medical Informatics Association, 4(5), 342–355. Https://Doi.Org/10.1136/Jamia.1997.0040342

[20]. ISO/IEC. (2013). Information Technology – Security Techniques – Information Security Management Systems – Requirements (ISO/IEC 27001:2013). International Organization For Standardization.

[21]. Kahindi, R., & Okello, D. (2020). The Role Of Digital Privacy Legislation In Kenya's Healthcare Sector. East African Journal Of Health And Information Systems, 2(1), 1–12.

[22]. Kim, K., & Johnson, M. E. (2021). The Role Of Information Governance In Healthcare Compliance And Safety. Journal Of Health Care Compliance, 23(4), 33–41.

[23]. Mutua, D. M. (2020). Challenges Of Implementing Health Information Systems In Kenya. Kenya Journal Of Health Informatics, 1(1), 20–30.

[24]. National Institute Of Standards And Technology (NIST). (2018). Framework For Improving Critical Infrastructure Cybersecurity. U.S. Department Of Commerce. Https://Www.Nist.Gov/Cyberframework