Journal of Applied Sciences, Information and Computing
Volume 7, Issue 1, April - May 2026
School of Mathematics and Computing, Kampala International University

ISSN: 3007-8903 https://doi.org/10.59568/JASIC-2026-7-1-04

Design and Analytical Validation of a Context-Aware Security Framework for Information-Sharing-Enabled Internet of Medical Things (IoMT) in Healthcare Systems

Arinaitwe Winfred[1], Kayeyo Margaret[2], Shefiu Olusegun Ganiyu[3], Michael Adawusi[4], Wanjiru Irene Muriithi[5]

[1,2,3,4,5] School of Mathematics and Computing, Kampala International University, Uganda
[1]winfred.arinaitwe@studmc.kiu.ac.ug,[2]margaret.kareyo@kiu.ac.ug
[3]ganiyu.shefiu@kiu.ac.ug, [4]michael.adawusi@kiu.ac.ug, [5]irene.muriithi@kiu.ac.ug

Abstract

The integration of Internet of Medical Things (IoMT) technologies has enhanced healthcare delivery through real-time data exchange and interoperable clinical systems. However, this integration simultaneously expanded cybersecurity risks associated with information sharing, especially in resource-constrained healthcare environments such as Nsambya and Rubaga Hospitals, where the research was conducted. This study aimed to design and analytically validate a context-aware security framework for information-sharing-enabled IoMT systems in healthcare. Guided by the Digital Health Security Architecture (DHSA) and Design Science Research (DSR), the study synthesized findings from prior framework evaluations and a comprehensive security requirements analysis to develop a multi-dimensional security framework. The proposed framework integrated four interdependent dimensions technical security functionalities, compliance and governance mechanisms, IT–clinical alignment, and socio-behavioral moderatorsdemonstrating full coverage of technical, organizational, behavioral, and contextual security requirements. Analytical and contextual validation indicated that the framework offered a robust, adaptable, and healthcare-oriented solution for securing IoMT-enabled healthcare systems, particularly in resource-constrained settings.

Keywords: Internet of Medical Things; Security Framework; Information Sharing; Digital Health Security Architecture; Healthcare Cybersecurity; Design Science Research.

1. Introduction

The digital transformation of healthcare systems has accelerated the adoption of Internet of Medical Things (IoMT) technologies that interconnect medical devices, wearable sensors, clinical information systems, and

Cloud-based platforms to support patient care. Through real-time data acquisition and information sharing, IoMT technologies enhance diagnostic accuracy, facilitate remote patient monitoring, and improve continuity of care (Islam et al., 2022). Secure information sharing is therefore a foundational capability for effective IoMT-enabled healthcare delivery.

Despite these benefits, healthcare IoMT ecosystems have become increasingly vulnerable to cybersecurity threats, including data breaches, ransomware attacks,

and device compromise incidents that directly threaten patient safety and service continuity (Coventry & Branley, 2023). These risks are exacerbated by device heterogeneity, constrained computational capacity, real-time operational dependency, and extensive human interaction. In resource-constrained healthcare environments, infrastructural limitations and weak cybersecurity governance further intensify these challenges.

Previous studies evaluating existing cybersecurity frameworks and deriving IoMT security requirements revealed significant gaps in healthcare contextualization, socio-behavioral integration, and clinical workflow alignment. Responding to these gaps, this study designs and analytically validates a context-aware security framework capable of operationalizing identified security requirements within healthcare IoMT ecosystems.

2. Materials and Methodologies

This study employed a Design Science Research (DSR) methodology to develop and validate a socio-technical security framework for information-sharing-enabled IoMT systems in Ugandan hospitals. The framework was informed by a comprehensive analysis of gaps in existing cybersecurity and healthcare informatics frameworks, an IoMT security requirements taxonomy, international standards (including IoTSF, ISO/IEC 27001, and HL7), and operational realities observed in resource-constrained healthcare settings. The design process followed a structured, iterative approach encompassing problem identification, objective definition, artifact development, demonstration, evaluation, and communication. Analytical and contextual validation strategies were applied to assess framework rigor, coherence, and applicability, ensuring both technical robustness and real-world operational relevance.

The study population consisted of healthcare providers and ICT personnel involved with IoMT systems across Lubaga National Referral Hospital and St. Francis Nsambya Hospital, representing approximately 500 potential participants. A stratified random sample of 201 respondents was selected to ensure balanced representation across clinical, technical, and managerial roles. Data collection employed a mixed-methods approach, including structured questionnaires to quantify perceptions of IoMT adoption and security practices, semi-structured interviews with key stakeholders to explore contextual and behavioral factors, and direct observation of IoMT devices and security protocols to triangulate findings. Reliability and validity were confirmed through pilot testing, with Cronbach's alpha values exceeding 0.7 for all constructs. Quantitative data were analyzed using ordered logistic regression, examining the influence of compliance mechanisms, security functionalities, IT–clinical alignment, and socio-behavioral moderators on secure IoMT adoption. Goodness-of-fit statistics and Nagelkerke R^2 were used to confirm model adequacy, while regression coefficients (β) highlighted the relative strength of predictors. Qualitative data underwent thematic content analysis to extract patterns related to staff perceptions, peer influence, and organizational culture, providing contextual insight to complement the statistical findings. Ethical considerations were rigorously observed, including IRB clearance, institutional permission, informed consent, and adherence to IoTSF guidelines on healthcare data confidentiality, ensuring a research design that is both scientifically robust and ethically sound.

3. Results

The primary result of this study is the design and analytical validation of a context-aware IoMT security framework structured around four interdependent dimensions. The technical security functionalities dimension addresses core requirements related to confidentiality, integrity, availability, authentication, secure interoperability, monitoring, and resilience.

The compliance and governance mechanisms dimension ensures regulatory alignment, accountability, auditability, and institutional oversight. The IT–clinical alignment layer integrates security controls with clinical workflows and service delivery objectives, while the socio-behavioral moderators dimension addresses human factors, security culture, usability, and behavioral compliance.

3.1 Objective: To develop a tailored security framework for Information Sharing-Enabled Internet of Medical Things.

This section focuses on the degree to which IT priorities are integrated with clinical operations, evaluated for their impact on patient care, and communicated to patients as part of service delivery improvements. Descriptive statistics on IT alignment to business goals were analyzed to assess how effectively IT strategies and initiatives support the overall mission and objectives of Lubaga and Nsambya hospitals. Understanding IT alignment is essential for the current study, as it highlights whether technological investments and IoMT deployments are strategically positioned to enhance healthcare outcomes. In the context of the study's purpose, these findings are vital since

IT alignment acts as an enabler that ensures the designed security framework is not only technically secure but also functionally responsive to institutional goals.

Table 4.1: showing descriptive statistics on IT alignment to business goals at selected Ugandan health institutions

Construct	No. of Items	Mean Range	Construct Average Mean	Average Std. Dev	Overall Interpretation
IT Alignment to Business Goals	7	2.65 – 4.27	3.34	0.75	Significant
High Performing Items	2 (AliBG1–3*)	3.58 – 4.27	3.84 (avg.)	≈0.76	Significant to Very Significant
Moderate Performing Items	5 (AliBG4–7)	2.65 – 3.22	2.97 (avg.)	≈0.74	Moderate influence
Response Pattern (Cross-Institutional)	—	Predominantly Neutral to Agree	—	Low dispersion (<1.0)	Stable and consistent perceptions

The findings demonstrate that IT alignment with institutional strategic goals in Lubaga and Nsambya Hospitals is statistically significant (M = 3.34, SD = 0.75), indicating substantive integration of IoMT systems within organizational planning and operational frameworks. Strong ratings for strategic alignment (AliBG1), investment prioritization (AliBG2), and particularly routine review of IT initiatives (AliBG3; M = 4.27) reflect governance maturity and structured oversight consistent with the IoTSF Security Compliance Framework. These results imply that digital health investments are not ad hoc but embedded within institutional performance architecture, thereby reinforcing secure information sharing, optimized resource allocation, and adaptive system monitoring. The very high endorsement of periodic review mechanisms further signals institutional capacity for iterative risk management and technological responsiveness—critical prerequisites for resilient IoMT ecosystems.

However, moderate ratings on cross-functional collaboration (AliBG4), impact measurement (AliBG5), clinical integration outcomes (AliBG6), and managerial feedback mechanisms (AliBG7) reveal structural gaps in performance evaluation, interdisciplinary coordination, and feedback institutionalization. These weaknesses suggest that while strategic intent and investment commitment are evident, operational consolidation remains uneven. From an IoTSF perspective, insufficient performance metrics and limited feedback loops may constrain long-term value realization, usability optimization, and proactive security strengthening. Consequently, strengthening evaluative analytics, enhancing IT–clinical collaboration, and institutionalizing leadership-driven feedback mechanisms would deepen strategic coherence and elevate IoMT deployment from aligned implementation to fully integrated, performance-accountable, and security-optimized digital health governance.

3.2Moderating variables (Socio-Economic Factors, Subjective Norms and Perceived Behavioral Control) at selected Ugandan health institutions.

Descriptive statistics on moderating variables were examined to determine how socio-economic factors, subjective norms, and perceived behavioral control influence the secure adoption and use of IoMT systems in Lubaga and Nsambya hospitals. These variables provide insight into the human and contextual dynamics that shape information sharing, including the effect of economic barriers, the role of social expectations, and the confidence of individuals in managing IoMT technologies. For this study, analyzing moderating variables is essential as they capture the socio-technical conditions under which the proposed security framework will operate. Their interpretation helps reveal whether staff and patients are adequately empowered, socially influenced, and economically supported to engage with IoMT systems securely, thereby complementing the technical and compliance dimensions of the framework.

Table 4.2: Showing moderating variables (Socio-Economic Factors, Subjective Norms, and Perceived Behavioral Control)

Construct	No. of Items	Mean Range	Construct Average Mean	Average Std. Dev	Overall Interpretation
Socio-Economic Factors (SEF)	4	2.63 – 3.79	3.09	0.76	Moderate influence
Subjective Norms (SN)	5	2.53 – 4.12	3.33	0.74	Significant influence
Perceived Behavioral Control (PBC)	5	3.09 – 4.35	3.79	0.73	Very Significant influence
Overall Moderating Variables	14	2.53 – 4.35	3.43	0.74	Significant
Response Pattern (Cross-Institutional)	—	Predominantly Neutral to Agree	—	Low dispersion (<1.0)	Stable and consistent perceptions

The findings reveal that moderating variables exert a statistically significant influence on information sharing-enabled IoMT usage (M = 3.43, SD = 0.7429), underscoring the centrality of socio-economic conditions, subjective norms, and perceived behavioral control in shaping secure digital health adoption. While respondents strongly acknowledged that socio-economic disparities affect IoMT effectiveness (MVSEF3), institutional integration of these realities into planning processes (MVSEF4) and provider awareness (MVSEF2) remained moderate, indicating partial contextual responsiveness. Similarly, subjective norms reflected a mixed behavioral climate: organizational culture and training endorsement (MVSN4, MVSN5) were strongly positive, yet peer-driven motivation (MVSN2) and perceived normative pressure were weak. These patterns suggest that although structural and cultural foundations for IoMT security exist, behavioral reinforcement mechanisms are not uniformly institutionalized. Consistent with the IoTSF Security Compliance Framework, effective IoMT governance must therefore extend beyond technical safeguards to embed socio-contextual inclusivity and normative strengthening within security design.

Perceived behavioral control emerged as comparatively robust, with high ratings for resource sufficiency (MVPBC3), manageable operational barriers (MVPBC4), and staff empowerment in influencing IoMT adoption (MVPBC5), indicating favorable operational readiness and psychological ownership. However, moderate perceptions regarding structured training adequacy (MVPBC2) and provider confidence (MVPBC1) signal the need for continuous capacity building and experiential security reinforcement. Collectively, these results imply that while Ugandan health institutions demonstrate promising infrastructural and motivational conditions for secure IoMT deployment, sustainable security performance depends on bridging awareness gaps, strengthening inclusive planning, and institutionalizing continuous behavioral enablement. In line with IoTSF principles, a context-sensitive, user-centered, and equity-informed security architecture is essential to transform IoMT implementation from functional adoption to resilient, compliance-driven digital health governance.

3.3 Information Sharing-Enabled IoMTS at selected Ugandan health institutions

Descriptive statistics on Information Sharing-Enabled IoMTs were analyzed to assess how securely and effectively medical data is exchanged within Lubaga and Nsambya hospitals. This section focuses on the mechanisms of data sharing, privacy and consent management, authentication practices, data governance, collaborative decision-making, adoption of emerging technologies, and ethical and legal considerations. Examining these indicators is crucial for the current study, as they highlight the extent to which hospitals have established secure, transparent, and patient-centered systems for IoMT-based information exchange. Understanding these patterns provides a basis for evaluating how well existing practices align with the proposed security framework and identifies areas that require strengthening to ensure safe and trusted medical data sharing in Uganda's healthcare institutions.

Table 4.3: Showing descriptive Statistics on Information Sharing-Enabled IoMTS at Selected Ugandan Health Institutions

Construct	No. of Items	Mean Range	Construct Average Mean	Average Std. Dev	Overall Interpretation
Data Sharing Mechanisms	3	2.59 – 4.27	3.71	0.68	Good to Excellent (Mixed Strength)
Privacy and Consent Management	4	2.55 – 3.10	2.83	0.76	Fair
Security and Authentication	4	2.64 – 4.32	3.66	0.72	Good to Excellent
Data Governance and Compliance	1	3.65	3.65	0.76	Good
Overall Information Sharing-Enabled IoMTS	12	2.55 – 4.32	3.46	0.72	Good and Statistically Significant

The study findings in **Table 4.3** indicate that the overall perception of information sharing-enabled IoMT functionalities was good (M = 3.50, SD = 0.7353), reflecting a large extent of agreement among healthcare providers at Lubaga Hospital and St. Francis Nsambya Hospital. This suggests that foundational IoMT features—secure data sharing, authentication, governance, compliance, and ethical oversight—are being positively experienced in practice. Within the IoTSF Security Compliance Framework, secure information exchange constitutes a central architectural objective; therefore, this favorable perception signals substantive institutional progress toward integrated and protected IoMT ecosystems in the studied hospitals.

Data Sharing Mechanisms

The findings reveal strong confidence in secure collaborative data exchange. Both ISDSM1 (M = 4.26, SD = 0.6708) and ISDSM2 (M = 4.27, SD = 0.6550) were rated excellent, indicating that healthcare providers perceive data sharing as both secure and interoperable. High agreement levels reflect trust in confidentiality safeguards and system integration. From an IoTSF perspective, this aligns with "Data in Transit" and Integration Assurance controls, which emphasize encryption, interoperability, and minimized duplication risks. These outcomes imply that core technical safeguards for data exchange are not only implemented but operationally effective in supporting collaborative care delivery.

However, ISDSM3 (M = 2.59, SD = 0.7267) was rated fairly satisfactory, indicating usability challenges in harmonizing data sharing mechanisms with best practices. High disagreement and neutrality rates suggest friction between security controls and user experience. According to the IoTSF Usability Security Design principle, secure systems must remain intuitive to prevent workarounds that could compromise compliance. Thus, while technical robustness is evident, user-centered refinement of sharing platforms remains necessary to optimize both security adherence and workflow efficiency.

Privacy and Consent Management

Privacy and consent processes present notable gaps. ISPCM1 (M = 2.89) and ISPCM2 (M = 2.78) were rated fairly satisfactory, indicating moderate uncertainty regarding transparency and consent withdrawal procedures. The predominance of neutral responses implies limited clarity or insufficient communication regarding patient rights. IoTSF privacy controls stress explicit, informed, and revocable consent mechanisms; therefore, these findings signal an urgent need to simplify consent forms, digitize opt-out systems, and improve patient-facing communication strategies.

Similarly, ISPCM3 (M = 3.10) reflects moderate staff training in privacy and consent management, while ISPCM4 (M = 2.55) highlights a communication deficit in informing patients about data use. Although privacy frameworks may exist structurally, their experiential implementation appears uneven. In line with IoTSF transparency requirements, institutions must institutionalize periodic privacy awareness campaigns and structured consent education programs to strengthen patient trust and regulatory compliance.

Security and Authentication

Security implementation presents a mixed pattern. Strong authentication practices (ISSA1; M = 2.64) were rated fairly satisfactory, indicating uncertainty or inconsistent awareness of authentication controls. This may reflect limited visibility of multi-factor authentication processes or uneven enforcement. Under IoTSF Secure Data Access standards, authentication consistency is non-negotiable; thus, facilities must reinforce technical safeguards alongside user education.

Conversely, regular security audits (ISSA2; M = 4.32) and clear communication of access policies (ISSA4; M = 4.30) were rated excellent. These findings demonstrate

institutional maturity in vulnerability management and governance communication. Routine auditing aligns directly with IoTSF Vulnerability Management standards, ensuring proactive identification of system weaknesses. Staff training in encryption and best practices (ISSA3; M = 3.36) was rated good but accompanied by high neutrality, indicating that while training exists, it may not be frequent or practically reinforced. Strengthening hands-on cybersecurity simulations and refresher workshops would enhance operational security confidence.

Data Governance and Compliance

Data governance practices are generally robust. ISDGC1 (M = 3.65) and ISDGC2 (M = 3.95) indicate that policies are present and audit-based compliance is actively pursued, including collaboration with external regulatory bodies. These findings reflect adherence to IoTSF Governance and Compliance domains, emphasizing policy review, accountability, and benchmarking.

Notably, ISDGC3 (M = 4.25) was rated excellent, suggesting strong clarity regarding staff roles and responsibilities in data management. This demonstrates organizational control maturity, as informed personnel are less likely to violate governance standards. Nonetheless, neutrality levels in ISDGC1 imply that broader staff involvement in policy review processes could enhance transparency and ownership.

Emerging Technologies

The adoption of emerging technologies is progressing steadily. ISET1 (M = 3.67) and ISET2 (M = 3.79) indicate institutional commitment to innovation and workforce development. Training on technological advancements appears relatively well institutionalized, consistent with IoTSF workforce development standards.

However, ISET3 (M = 3.49) reveals moderate confidence in post-implementation evaluation and feedback mechanisms. High neutrality suggests limited staff awareness of evaluation processes. IoTSF innovation lifecycle guidance underscores the importance of structured feedback loops; thus, strengthening participatory technology assessments would enhance both performance optimization and cybersecurity resilience.

Ethical and Legal Considerations

Ethical integration reveals contrasting results. ISEL1 (M = 2.67) was rated fairly satisfactory, indicating perceived gaps in embedding ethical considerations directly into routine data-sharing practices. The high neutrality and disagreement levels imply either weak enforcement or limited visibility of ethical audits. Under the IoTSF Ethical Governance pillar, privacy, fairness, and justice must be operationalized—not merely policy-based—within digital health environments.

Conversely, ethical training (ISEL2; M = 4.07) and proactive management of ethical dilemmas (ISEL3; M = 4.12) were rated excellent, demonstrating strong institutional commitment to ethical education and consent integrity. Regular review and communication of ethical guidelines (ISEL4; M = 3.56) were rated good but suggest room for more interactive engagement forums.

Overall Interpretation

Overall, the findings demonstrate that information sharing-enabled IoMT systems are substantially supported across the participating hospitals (M = 3.50), with particular strengths in interoperability, security audits, governance clarity, and ethical training. These results strongly align with the IoTSF Security Compliance Framework's emphasis on secure interoperability, structured governance, continuous auditing, and workforce empowerment.

However, weaknesses persist in usability design, consent transparency, authentication visibility, and the operationalization of ethical principles in day-to-day practice. For institutions such as Lubaga Hospital and St. Francis Nsambya Hospital, strengthening human-centered design, enhancing patient communication, reinforcing authentication consistency, and institutionalizing participatory ethical oversight will be critical. A comprehensive IoTSF-aligned approach must therefore integrate both technical safeguards and socio-organizational reforms to ensure secure, transparent, and sustainable IoMT-enabled information sharing within Uganda's healthcare system.

3.4 Checklist results

The checklist results provide an additional layer of validation by assessing the practical implementation of security functionalities, compliance measures, IT alignment, and moderating variables across Nsambya and Lubaga Hospitals. Unlike the survey and interviews, the checklist directly examined whether specific security practices and protocols were in place within the institutions. By capturing responses on items such as device, network, and data security, compliance with regulations, IT-business integration, and patient-centered safeguards, the checklist results reveal the operational realities of IoMT adoption. These findings not only confirm the survey data but also expose critical gaps and strengths, thereby offering a practical benchmark for designing a robust security framework that ensures safe and effective information sharing in Ugandan healthcare institutions.

Showing checklist results (Table 4.4)

Factor	No. of Items	Lubaga Yes (%)	Nsambya Yes (%)	Overall Avg Yes (%)	Interpretation
Security Functionalities	9	80%	72%	76%	Strong institutional security controls with minor procedural gaps
Compliance	6	68%	62%	65%	Moderate compliance; gaps in risk assessment and continuity planning
IT Alignment	3	80%	77%	78%	Strong strategic IT alignment with patient-centered focus
Moderating Variables	9	50%	58%	54%	Moderate socio-behavioral and access-related support structures
Information Sharing – IoMTs	21	74%	74%	74%	Generally robust governance and transparency mechanisms

From the checklist data provided for Lubaga and Nsambya Hospitals, several important findings emerge regarding institutional preparedness for information sharing-enabled IoMTs.

First, both hospitals demonstrate partial but uneven adoption of security functionalities. Most respondents indicated that devices, networks, and data systems are secured through identifiers, firewalls, and encryption, but gaps remain in critical practices such as regular patching, reporting suspicious behavior, and consistent two-factor authentication. This inconsistency implies that while core security mechanisms exist, implementation lacks uniform enforcement across departments. For IoMT adoption, this poses risks of vulnerabilities that could compromise sensitive patient data. Second, under compliance, responses show mixed results. Although both hospitals reported adherence to data protection regulations and collaborations with regulatory bodies, staff training on compliance standards is less consistent. Risk assessments and business continuity planning were recognized in some instances but were not universal, indicating that resilience-building still needs institutional strengthening. The implication is that compliance mechanisms exist but require regular updating and integration into daily practices, especially through staff training and simulation drills.

Third, IT alignment with business goals showed recognition of Information Technology's role in supporting hospital missions and patient care. However, fewer respondents confirmed that patients are systematically informed of IT improvements. This suggests that while IT strategies are aligned institutionally, their translation into patient-centered communication is weaker. Effective IoMT adoption requires not only technical integration but also patient awareness to build trust.

Fourth, the moderating variables highlight socio-behavioral gaps. Although there was acknowledgment of socio-economic barriers and a culture of security awareness among staff, fewer provisions were reported for supporting vulnerable populations or systematically encouraging patients to report concerns. Similarly, staff-patient communication on security issues appeared inconsistent. This indicates that socio-economic readiness and patient empowerment are underdeveloped, limiting the inclusiveness of IoMT adoption. Finally, information-sharing mechanisms such as informed consent, data anonymization for research, and transparency of third-party data-sharing agreements were inconsistently applied across both hospitals. Robust authentication and data governance frameworks were often affirmed, but regular audits and mechanisms for patient feedback were not consistently observed. While ethical and legal considerations were broadly recognized, practical application such as addressing patient-raised concerns remains partial.

Implications for the study suggests that Lubaga and Nsambya hospitals are in a transitional phase of IoMT readiness. They possess foundational technical and compliance structures but lack uniform implementation, staff engagement, and patient-centered practices. For the purpose of developing a security framework, this underscores the need for a holistic, socio-technical approach that integrates:

i. Stronger enforcement of technical safeguards (patching, authentication, monitoring).
ii. Continuous compliance training and incident preparedness.
iii. Alignment of IT with both clinical goals and patient communication.
iv. Addressing socio-economic barriers through targeted support for vulnerable groups.
v. Strengthening governance with transparent, ethical, and participatory data-sharing mechanisms.

Altogether, the results affirm the study's rationale: To design a security framework that not only enforces technical protections but also embeds compliance, socio-

behavioral readiness, and patient engagement as central pillars for secure IoMT adoption in Ugandan hospitals.

3.5 Associations between demographic characteristics, security frameworks, and IoMT adoption in Lubaga and Nsambya Hospitals

This section presents an in-depth statistical analysis exploring associations between demographic characteristics and respondents' experiences with Information Sharing-Enabled IoMTs in Lubaga and Nsambya Hospitals. Using the Chi-square test at a 0.05 significance level, the study examined whether variables such as hospital affiliation, gender, education level, and professional role influenced exposure to IoMT systems. The results revealed mixed outcomes where gender showed a significant relationship, particularly in Nsambya Hospital, while other variables did not. Following this, Spearman's Rank Correlation was used to assess relationships between security framework components and IoMT adoption, and finally, Ordinal Regression was applied to model the predictive power of these security factors. Collectively, these analyses provide a foundation for developing a robust, context-specific security framework.

3.5.1 Chi-square test

Under this section, Chi-square Test analysis was carried out to examine associations between demographic characteristics and respondents' experience with Information Sharing-Enabled IoMTs in Lubaga and Nsambya Hospitals. Using an alpha threshold of 0.05, the chi-square tests assessed whether hospital affiliation, gender, education, and professional role significantly influenced IoMT exposure. As shown in Table 4.5.1**,** the results revealed mixed outcomes, with some variables showing significant relationships while others did not.

Table 4.5: Showing Chi-square test results

The following chi-square tests were conducted to assess associations between demographic variables and experience with IoMTs. The standard significance threshold of $p < 0.05$ was used to determine statistical significance.

Categorical factors/Variable Pair	Chi² Statistic	df	p-value *(α ≤ 0.05)*	Conclusion
Hospital × IoMTS_Experience	0.0008	1	0.9769	Not Significant
Gender × IoMTS_Experience	10.7599	3	0.0131	Significant
Gender × IoMTS_Experience- Lubaga	7.0420	3	0.0706	Not Significant
Gender × IoMTS_Experience- Nsambya	9.4606	3	0.0238	Significant
Education × IoMTS_Experience	1.9806	4	0.7393	Not Significant
Role × IoMTS_Experience	7.3344	4	0.1192	Not Significant

The results presented in Table **4.5**; Chi-square test results provide important insights into the association between various demographic characteristics and respondents' experience with Information Sharing-Enabled Internet of Medical Things (IoMTs) in Lubaga and Nsambya Hospitals. The chi-square tests were conducted using a standard alpha level of 0.05 to determine statistical significance.

Firstly, the relationship between Hospital and IoMT experience yielded a chi-square statistic of 0.0008**,** with a p-value of 0.9769**,** indicating no statistically significant association. This result implies that the proportion of respondents who had experience with IoMTs was relatively consistent across both hospitals. Therefore, institutional affiliation (whether Lubaga or Nsambya) does not appear to influence exposure to IoMTs, suggesting uniformity in technological access or deployment strategies across the two facilities. In contrast, a statistically significant association was found between Gender and IoMT experience, with a chi-square value of 10.7599 and a p-value of 0.0131, which is well below the 0.05 threshold. This finding implies that IoMT experience is gender-dependent, with certain gender groups (likely male or female staff) having had greater exposure or access to IoMT technologies. This raises important considerations for equity and inclusivity in the implementation and training processes related to IoMTs in health institutions.

Medical Things (IoMTs) in Lubaga and Nsambya Hospitals. The chi-square tests were conducted using a

standard alpha level of 0.05 to determine statistical significance.

Firstly, the relationship between Hospital and IoMT experience yielded a chi-square statistic of 0.0008**,** with a p-value of 0.9769**,** indicating no statistically significant association. This result implies that the proportion of respondents who had experience with IoMTs was relatively consistent across both hospitals. Therefore, institutional affiliation (whether Lubaga or Nsambya) does not appear to influence exposure to IoMTs, suggesting uniformity in technological access or deployment strategies across the two facilities. In contrast, a statistically significant association was found between Gender and IoMT experience, with a chi-square value of 10.7599 and a p-value of 0.0131, which is well below the 0.05 threshold. This finding implies that IoMT experience is gender-dependent, with certain gender groups (likely male or female staff) having had greater exposure or access to IoMT technologies. This raises important considerations for equity and inclusivity in the implementation and training processes related to IoMTs in health institutions.

Further analysis by hospital revealed contrasting results. For Lubaga Hospital**,** the relationship between Gender and IoMT experience was not statistically significant **(**χ^2 = 7.0420, p = 0.0706**),** although the p-value was near the threshold, suggesting a potential trend that might become significant with a larger sample size or additional variables. Meanwhile, Nsambya Hospital displayed a significant association between Gender and IoMT experience (**χ^2** = 9.4606, p = 0.0238), indicating that gender-based disparities in IoMT access or training are more pronounced in that facility. These differences underscore the need for hospital-specific interventions and policy considerations to ensure gender-equitable participation in IoMT systems, as advocated in the IoTSF Security Compliance Framework**,** which emphasises inclusivity and balanced user access. On the other hand, the relationship between Education level and IoMT experience **was** not significant **(**χ^2 = 1.9806, p = 0.7393**)**, suggesting that formal educational attainment does not significantly influence whether one has interacted with IoMT systems. This could imply that IoMT exposure in these hospitals may be more dependent on roles, departmental assignments, or institutional policies than academic qualifications.

Lastly, the relationship between Professional Role and IoMT experience also failed to reach statistical significance (**χ^2 =** 7.3344, p = 0.1192**),** indicating that job role (e.g., doctor, nurse, lab officer) was not a determining factor in access to or experience with IoMTs in the current sample. However, like the Lubaga gender comparison, the p-value here is relatively close to 0.05, suggesting that more nuanced analysis or larger samples might uncover emerging patterns. In summary, the chi-square results highlight gender and particularly within Nsambya Hospital as a significant factor influencing IoMT experience. Meanwhile, hospital affiliation, education level, and professional role did not yield statistically significant associations. These findings suggest the importance of addressing gender disparities and exploring deeper organizational or cultural factors that may shape IoMT adoption in Uganda's healthcare institutions.

4.5.2 Spearman's Rank correlation

Under this section Spearman's Rank Correlation examined associations between security framework factors and IoMT adoption, revealing significant correlations across security functionalities, compliance, IT alignment, and moderating variables. As shown in Table 4.12, coefficients ranged from weak to strong, with $p \leq 0.05$ confirming significance. These findings imply that IoTSF-aligned frameworks integrating technical controls, compliance, and socio-behavioural enablers can strengthen secure IoMT-enabled information sharing in Lubaga and Nsambya hospitals.

Table 4.6: Spearman Correlation Coefficients (ρ) results

Relationship	Spearman ρ	Strength	p ≤ .05	Direction	Interpretation
Security Functionalities ↔ IoMTS	0.252*	Weak–Moderate	Yes	Positive	Significant positive association
Compliance ↔ IoMTS	0.224*	Weak–Moderate	Yes	Positive	Significant positive association
IT Alignment ↔ IoMTS	0.072	Weak	No	Positive	Non-significant weak association
Moderating Variables ↔ IoMTS	0.218*	Weak–Moderate	Yes	Positive	Significant positive association
Security Framework (Composite) ↔ IoMTS	0.345*	Moderate	Yes	Positive	Significant moderate positive association

Correlation is significant at 0.05 level (2-tailed). Security framework correlated with security (ρ=0.605*), compliance (ρ=0.564*), IT alignment (ρ=0.467*), IoMT (ρ=0.345*); weak moderating links (ρ=0.068, -0.006).

The Spearman's Rank Correlation analysis revealed several significant associations among the study variables, providing deeper insight into how security frameworks influence information sharing-enabled IoMTs in Ugandan hospitals. To begin with, a strong and positive correlation was found between the security framework (Total_SecFrame) and security functionality (Total_SecFun) ($\rho = 0.605$, $p < 0.05$). This finding implies that when robust security frameworks are established, the functionality of IoMT devices in securing patient information improves significantly. Similarly, the security framework also correlated positively with compliance ($\rho = 0.564$, $p < 0.05$) and IT alignment ($\rho = 0.467$, $p < 0.05$), suggesting that well-developed security frameworks encourage adherence to regulatory standards while ensuring that IT strategies and policies are aligned with institutional goals for safe IoMT deployment.

In addition, the correlation between the security framework and IoMTs implementation ($\rho = 0.345$, $p < 0.05$) was positive and significant, indicating that security measures play a central role in enhancing effective IoMT adoption. This finding aligns with the IoTSF Security Compliance Framework, which emphasizes that data-sharing systems must be underpinned by security-by-design to build trust and efficiency in healthcare environments. Moreover, the results showed that IoMTs implementation (Total_IoMTS) had significant positive correlations with security functionality ($\rho = 0.252$, $p < 0.05$), compliance ($\rho = 0.224$, $p < 0.05$), and moderating variables such as user behavior and awareness ($\rho = 0.218$, $p < 0.05$). This implies that secure, compliant practices and human factors like awareness and training contribute directly to the successful integration of IoMTs. Taken together, these correlations confirm that security frameworks do not operate in isolation; rather, they strengthen compliance, enhance security functions, align IT with organizational objectives, and foster positive human engagement. Consequently, the findings demonstrate that institutions such as Lubaga and Nsambya Hospitals can significantly improve IoMT-enabled information sharing by embedding IoTSF-aligned frameworks that emphasize technical controls, compliance monitoring, and continuous user training. This holistic approach ensures that security not only safeguards data but also drives effective healthcare innovation through IoMT adoption.

4.5.3 Regression analysis and modeling

Ordinal Regression analysis was performed to predict the influence of Security Framework factors (independent variables) on Information Sharing-Enabled IoMTs (dependent variable) within Lubaga and Nsambya Hospitals. After conducting the preliminary tests, namely the reliability test, Chi-square test, and Spearman's Rank correlation, the relevant factors retained for regression analysis included the core dimensions of the security framework: Security Functionality (SecFun), Compliance (Comp), IT Alignment (ITAlign), and Moderating Variables (ModV). These factors were considered crucial as they were found to significantly correlate with IoMT implementation during preliminary analysis. From the Ordinal Regression results, the model was validated using the standard parameters, including Model Fitting Information, Goodness-of-Fit test, Pseudo R-square Statistics, Parameter Estimate values, and the Test of Parallel Lines. Collectively, the measurement values generated under these parameters explained how well the regression model fit the dataset and confirmed the predictive influence of the identified security framework factors on IoMT-enabled information sharing.

Showing Ordinal Regression Analysis Results (Table 4.5.2)

Dimension	β	p ≤ .05	Nagelkerke R^2	Model Fit (χ^2, p)	Overall Interpretation
Security Functionalities → IoMTs	0.197	0.000 (Yes)	0.410	χ^2=204.319, p=.000 (Significant)	Strong positive and statistically significant predictor; good deviance fit
Compliance → IoMTs	0.197	0.000 (Yes)	0.276	χ^2=124.813, p=.000 (Significant)	Moderate positive and statistically significant predictor; adequate fit
IT Alignment → IoMTs	0.087	0.055 (Marginal)	0.276	χ^2=87.562, p=.054 (Borderline)	Weak to marginal predictor; borderline model significance
Moderating Variables → IoMTs	0.144	0.000 (Yes)	—	Model significant at p=.000	Significant moderating effect on IoMT implementation

The ordered-logit model predicting Information Sharing-Enabled IoMT adoption in Lubaga Hospital and St. Francis Nsambya Hospital demonstrated robust statistical validity, with a significant chi-square improvement over the intercept-only model ($\chi^2 = 124.813$, df = 51, $p < .05$) and non-significant Goodness-of-Fit statistics (Pearson and Deviance, $p = 1.000$), confirming accurate representation of the observed data.

The Nagelkerke R^2 of 0.276 indicates that nearly 28% of the variance in IoMT adoption is explained by the model, a notable outcome given the complexity of socio-technical and organizational behaviors in healthcare. Among the predictors, Compliance and Security Functionalities emerged as the most influential, with highly significant positive coefficients ($\beta = 0.197$, $p < .05$), demonstrating that adherence to standards, collaboration, resilience, risk management, and implementation of device-, network-, and data-level safeguards are critical determinants of secure IoMT adoption. Moderating variables encompassing socio-economic factors, subjective norms, and perceived behavioral control also showed significant positive associations ($\beta = 0.144$, $p < .05$), illustrating that technical safeguards alone are insufficient; staff perceptions, peer expectations, and contextual readiness substantially influence the practical uptake and secure use of IoMT systems. Compliance sub-dimensions further reinforced socio-economic and normative readiness, highlighting the dual role of compliance as both a procedural enabler and a cultural legitimizer within healthcare institutions.

These findings carry significant implications for the design of a context-specific IoMT security framework. Primarily, the framework must embed strong technical and procedural safeguards as its core, ensuring device-, network-, and data-level protection while operationalizing robust compliance structures. Equally critical is the integration of socio-behavioural interventions, including targeted training, norm-building, and empowerment strategies, which address behavioural, peer, and socio-economic influences on secure system use. IT alignment, although contributing positively to socio-economic readiness ($\beta = 0.095$, $p < .05$), plays a secondary facilitative role and should support rather than dominate the framework. Collectively, these results underscore the necessity of a socio-technical approach that harmonizes institutional policies, technical safeguards, and behavioural enablers, ensuring that IoMT adoption in Ugandan hospitals is not only procedurally compliant and technically secure but also practically embraced by staff. Such a dual focus directly advances the study's objective of constructing a security framework that enhances both institutional readiness and the operational effectiveness of information sharing-enabled IoMTs within complex healthcare environments.

4. Discussions

The study findings underscore that secure information sharing in Information of Medical Things (IoMT) ecosystems is intrinsically a socio-technical phenomenon, where technical safeguards alone are insufficient to ensure effective adoption. Compliance mechanisms and security functionalities emerged as the strongest predictors of IoMT adoption, demonstrating that adherence to standards, risk management practices, and device-, network-, and data-level security directly shape institutional readiness for secure information sharing. These results align with the principles of the IoTSF Security Compliance Framework, which emphasizes that technical protections must be embedded within robust governance structures to mitigate vulnerabilities and support operational continuity (IoTSF, 2022). Furthermore, the significant influence of socio-behavioural moderators—including socio-economic factors, subjective norms, and perceived behavioural control—highlights that human perception, peer influence, and contextual readiness play a decisive role in whether security mechanisms translate into practical, everyday use (Ajzen, 1991; Venkatesh et al., 2012). The empirical evidence thus suggests that secure IoMT deployment cannot be reduced to a checklist of technical solutions; rather, it requires an integrated framework that recognizes the interplay between technology, organizational culture, and human behaviour.

A second notable implication of the findings relates to the integration of compliance sub-dimensions with social and normative factors. Standards, collaboration, resilience, and risk management were consistently associated with socio-economic readiness and peer acceptance, while their influence on perceived behavioural control was weaker. This indicates that compliance acts not only as a procedural enabler but also as a cultural legitimizer, fostering normative endorsement and reinforcing staff confidence in adopting secure IoMT practices. The results are consistent with prior literature on institutional theory, which posits that formal regulations and governance mechanisms gain effectiveness when internalized within organizational culture (Scott, 2014). Consequently, any security framework designed for Ugandan hospitals, such as Lubaga and Nsambya, must embed compliance structures as central pillars that simultaneously reinforce technical security and cultivate a culture of trust, accountability, and shared responsibility among healthcare professionals.

The findings also reveal the critical role of human-cantered design and IT–clinical alignment in shaping practical IoMT adoption. While IT alignment exhibited a smaller, marginally significant effect, its positive association with socio-economic readiness underscores its role as a facilitating enabler rather than a primary driver of secure use. Effective alignment ensures that digital health initiatives are synchronized with hospital missions and care delivery objectives, thereby enhancing the perceived relevance of security measures and reducing operational friction (Henderson & Venkatraman, 1993). In this light, frameworks that neglect the IT–clinical interface risk implementing technically robust solutions that fail to achieve practical

uptake or generate user compliance. By incorporating an explicit alignment layer alongside socio-technical safeguards, the proposed framework addresses this gap, providing a more holistic approach than conventional models that focus narrowly on either technical or governance aspects of security.

Finally, the framework's emphasis on incremental implementation, contextual adaptability, and human-cantered security is particularly relevant for resource-constrained healthcare settings. The data indicate that staff empowerment, training, and user engagement are essential for both effective IoMT adoption and sustainable security practice, reflecting the necessity of designing for operational realities rather than assuming technological abundance (Greenhalgh et al., 2017). By integrating socio-behavioral moderators and feedback mechanisms into the security framework, institutions can iteratively adapt technical safeguards, governance policies, and training programs to real-world workflows, patient demographics, and socio-economic constraints. This approach ensures that security measures are not only technically compliant but also culturally and operationally feasible, fostering long-term sustainability, user ownership, and trust in IoMT-enabled healthcare delivery systems within Ugandan hospitals.

5. Conclusion

The study conclusively demonstrates that secure adoption of information sharing-enabled IoMTs in Ugandan healthcare institutions, specifically Lubaga Hospital and St. Francis Nsambya Hospital, is a multidimensional socio-technical endeavor. Empirical evidence from the ordered-logit model confirms that both technical and governance-based safeguards, encompassing device-level, network-level, and data-level security, alongside robust compliance mechanisms, are indispensable for achieving high levels of secure information exchange. Compliance sub-dimensions—including standards, collaboration, resilience, and risk management—were shown to be critical not only in ensuring procedural adherence but also in shaping socio-cultural acceptance, peer endorsement, and normative legitimacy among healthcare providers. Consequently, a security framework for IoMT cannot be conceived solely as a technical blueprint; it must also operationalize governance legitimacy and foster an organizational culture of trust, accountability, and shared responsibility.

In addition to technical and governance considerations, socio-behavioral moderators were identified as significant determinants of IoMT adoption. Socio-economic factors, subjective norms, and perceived behavioral control exerted measurable influence on the effectiveness and uptake of security functionalities, highlighting that staff perceptions, peer influence, and contextual readiness are crucial in translating security mechanisms into sustained practice. The study demonstrates that human-centered interventions, including structured training, awareness programs, and normative reinforcement, are essential complements to technical safeguards, effectively bridging the gap between theoretical compliance and practical implementation. This reinforces the notion that secure IoMT deployment is inherently socio-technical, requiring integrated strategies that account for human, environmental, and organizational realities.

The findings further underscore the necessity of IT–clinical alignment and incremental, context-sensitive implementation strategies. While IT alignment had a secondary influence compared to compliance and security functionalities, its positive effect on socio-economic readiness indicates that harmonizing digital health initiatives with institutional objectives enhances the perceived relevance of security measures and facilitates user compliance. In resource-constrained healthcare environments, the framework's emphasis on adaptability, incremental rollout, and human-centered design ensures that security interventions are both feasible and sustainable, mitigating the risk of technological misalignment or underutilization. By embedding these considerations into the IoMT security framework, institutions can achieve a balance between operational feasibility, technical robustness, and behavioral adherence.

Ultimately, this study establishes a foundation for a context-specific, socio-technical IoMT security framework that integrates compliance, technical safeguards, human behavior, and organizational alignment. The framework advances both theory and practice by demonstrating that effective information-sharing-enabled IoMT adoption requires the simultaneous cultivation of procedural rigor, technical resilience, and socio-behavioral legitimacy. For Ugandan hospitals, this integrated approach ensures that security mechanisms are not only operationally robust but also socially accepted, culturally aligned, and sustainable, thereby providing a replicable model for other resource-constrained healthcare settings seeking to strengthen IoMT-enabled digital health systems.

Recommendations

Based on the findings, it is recommended that Lubaga Hospital and St. Francis Nsambya Hospital, as well as similar healthcare institutions in Uganda, adopt a holistic, socio-technical approach to IoMT security that integrates technical safeguards, governance structures, and human behavioral interventions. Firstly, hospitals should strengthen compliance and security functionalities by enforcing device-level, network-level, and data-level protections, coupled with systematic risk management and resilience protocols. Compliance should not merely serve as a procedural requirement but should be operationalized as a cultural driver that enhances normative acceptance, peer endorsement, and institutional legitimacy of IoMT adoption (IoTSF,

2022). Regular audits, clear communication of policies, and continuous updates of governance standards are crucial to maintaining accountability and ensuring adherence to both local regulations and international best practices.

Secondly, healthcare institutions should prioritize socio-behavioral interventions to complement technical measures. Training programs, peer-led norm-building initiatives, and awareness campaigns should be institutionalized to reinforce staff confidence, perceived behavioral control, and the social legitimacy of IoMT usage. Particular attention should be given to bridging socio-economic disparities in technology access and literacy among staff and patients, ensuring that digital health solutions are inclusive and equitable. Embedding feedback mechanisms, scenario-based exercises, and participatory design approaches will help tailor interventions to user needs, thereby enhancing both usability and compliance.

Thirdly, incremental and context-sensitive IT alignment should be pursued to harmonize IoMT initiatives with organizational strategic goals. Hospitals should integrate IoMT planning with institutional objectives, ensuring that resource allocation, clinical workflows, and digital health strategies are synchronized. This alignment serves as a facilitating enabler that reinforces staff engagement and operational relevance without overshadowing the primacy of compliance and technical safeguards.

Finally, it is recommended that healthcare institutions institutionalize ethical and privacy practices as core pillars of IoMT deployment. Transparent consent processes, clear withdrawal procedures, proactive ethical audits, and regular staff training in legal and ethical frameworks will strengthen patient trust, safeguard sensitive information, and ensure legal compliance. Integrating these measures within the security framework will create a sustainable, human-centered digital health ecosystem that balances technical robustness with ethical, social, and operational considerations. Collectively, these recommendations provide a comprehensive roadmap for the development of a **con**text-specific, socio-technical IoMT security framework that is adaptable, scalable, and capable of supporting secure, effective, and equitable information sharing in resource-constrained healthcare environments.

References

[1] Ajzen, I. (1991). *The theory of planned behavior*. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

[2] Baxter, G., & Sommerville, I. (2019). Socio-technical systems. ACM Computing Surveys, 51(4), 1–38.

Coventry, L., & Branley, D. (2023). Cybersecurity in healthcare. Health Informatics Journal, 29(1), 1–15.

[3] Furnell, S., & Shah, J. N. (2023). Human factors in healthcare cybersecurity. Computers & Security, 123, 102915.

[4] Greenhalgh, T., Wherton, J., Papoutsi, C., Lynch, J., Hughes, G., A'Court, C., … & Shaw, S. (2017). Beyond adoption: A new framework for theorizing and evaluating nonadoption, abandonment, and challenges to the scale-up, spread, and sustainability of health and care technologies. *Journal of Medical Internet Research, 19*(11), e367. https://doi.org/10.2196/jmir.8775

[5] Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal, 32*(1), 4–16. https://doi.org/10.1147/sj.323.0004

[6] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105.

IoTSF. (2022). *IoT Security Foundation: Security compliance framework*. IoT Security Foundation. https://www.iotsecurityfoundation.org

[7] Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2022). The Internet of Things for healthcare. IEEE Access, 10, 12589–12625.

[8] Scott, W. R. (2014). *Institutions and organizations: Ideas, interests, and identities* (4th ed.). SAGE Publications.

[9] Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36*(1), 157–178. https://doi.org/10.2307/41410412