EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 10||pp 22-36||October||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

Examination of Data Protection Ethical Guidelines Adopted by Kenyatta National Hospital to Protect Its Healthcare System

Stephen Okongo Ario[1*], Dr. Jecton Tocho, PhD[2], Mrs. Jenu John[3]
[123]Department of Computer Science, Kenya Methodist University
*Corresponding author email: ariostephen@gmail.com

Accepted: 11 August 2025 || Published: 02 October 2025

Abstract

The study examined data protection ethical guidelines adopted by Kenyatta National Hospital to protect its healthcare system. This study adopted a descriptive research design to examine cybersecurity threats and countermeasures within the healthcare sector, focusing specifically on Kenyatta National Hospital (KNH). The target population includes all staff categories involved in patient care, information management, and IT infrastructure. The accessible population consisted of 5,983 staff who were available and consented to participate in the study during the data collection period. A stratified random sampling technique was deemed the most appropriate. The sample size of 370 respondents was determined based on a population of 4,933 staff members relevant to the study (clinical staffs, ICT, and health records and admin staffs) out of an approximate total population of 5,983(total staffs at KNH). Across the five key items assessed, the overall mean is 3.94, with a standard deviation of 1.17 and a variance of 1.38. These results indicate a general agreement among respondents that KNH upholds ethical standards in managing patient information, with moderate variability suggesting some differences in perceptions regarding the consistency and effectiveness of these practices. The item "KNH has a documented code of ethics that defines how patient data should be accessed, stored, shared, and protected to ensure responsible use" recorded a mean score of 3.83 (SD 1.17, Var 1.36). This reflects agreement that a formal ethical framework exists to guide responsible data management, although the moderate variability points to some differences in how clearly this code is understood or implemented across the hospital. The conclusion drawn is that ethical norms play a foundational role in sustaining secure digital environments in healthcare. When these guidelines are well-communicated and embedded in practice, they promote responsible system use and help bridge gaps left by technological or legal limitations. Thus, a values-driven approach to cybersecurity is critical for institutional resilience. Ethical data protection guidelines were identified as the strongest predictor of an effective cybersecurity framework. However, inconsistencies in training and partial enforcement were noted. The study recommends that KNH should institutionalize ethical guidelines by embedding them into everyday workflows, onboarding protocols, and performance appraisals. Comprehensive, role-specific training should be offered consistently across all departments. Furthermore, the management should develop an e-learning module on healthcare data ethics, tailored to job functions (clinicians, IT staff, and administrative personnel), and make certification mandatory on an annual basis.

Keywords: *Data Protection Ethical Guidelines, Kenyatta National Hospital, Healthcare System*

EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 10||pp 22-36||October||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

How to Cite: Ario, S. O., Tocho, J. T., & Jenu, J. (2025). Examination of Data Protection Ethical Guidelines Adopted by Kenyatta National Hospital to Protect Its Healthcare System. *Journal of Information and Technology, 5*(10), 22-36.

1. Introduction

While legal frameworks establish the parameters of data governance, ethics addresses the values underpinning how data should be handled. Ethical data protection ensures that patient information is treated with respect for privacy, confidentiality, informed consent, and autonomy, regardless of the presence of technical controls (Beauchamp & Childress, 2019). In healthcare, ethical breaches not only erode patient trust but may lead to harmful consequences, including stigmatization, discrimination, or compromised treatment outcomes (Shachar et al., 2020). In the era of digital health, ethical concerns have expanded. The use of electronic health records (EHRs), cloud storage, biometric verification, and health data analytics introduces new risks, such as unauthorized third-party access, data commodification, and systemic surveillance without consent (Maher & Kruger, 2022). Therefore, ethical safeguards must evolve to match the complexity of emerging technologies.

Kenya's Data Protection Act (2019) includes several ethically relevant principles such as purpose limitation, data minimization, accuracy, and accountability (Office of the Data Protection Commissioner, 2022). However, a national assessment by CIPIT (2021) reported that over 68% of public healthcare workers had no formal training in ethical data handling, and only a small minority understood key patient rights under the Act. These findings suggest that while Kenya has the legislative tools, its ethical data governance remains weakly institutionalized in practice. Within KNH, ethical vulnerabilities are apparent in both system design and institutional culture. According to KNH's own internal evaluations (KNH Strategic Plan, 2018–2023), most departments lack formal guidelines on consent for electronic data, and there is no standardized process for controlling interdepartmental access to patient records.

This often results in sensitive patient data being shared without proper authorization, especially in emergency settings where decisions are made quickly (Willis, 2015). Moreover, digital platforms such as LIS and EMRs at KNH do not consistently implement audit trails or role-based access controls, which are critical for accountability (Kimani & Wanjiru, 2023). Mutinda and Ongus (2020) also report that KNH has not yet established a functional data ethics committee, nor does it conduct regular ethical audits of its digital systems. Given these challenges, this study examines the extent to which ethical principles of data protection have been adopted at KNH and whether these principles are embedded in staff training, digital policy, and patient communication. By addressing this issue, the study contributes to its broader aim of building a socio-technical cybersecurity framework that is not only legally compliant but also ethically sound.

1.1 Problem Statement

The digitization of healthcare systems has brought significant advancements in the management of patient information, service delivery, and operational efficiency. However, it has also introduced complex cybersecurity risks that threaten the confidentiality, integrity, and availability of sensitive health data. Globally, hospitals have become prime targets for cyberattacks, with incidents of data breaches, ransomware, and unauthorized access increasing in frequency and sophistication (Ghafur et al., 2022). In the Kenyan context, the growing

adoption of electronic health records and interconnected medical systems has heightened the urgency for robust cybersecurity frameworks, particularly in large public hospitals such as Kenyatta National Hospital (KNH).

Despite the enactment of the Kenya Cybercrime Act and the presence of ethical guidelines related to data protection, recent observations and reports suggest that public healthcare institutions remain vulnerable to cyber threats. These vulnerabilities are often exacerbated by limited technical infrastructure, inconsistent policy enforcement, insufficient staff training, and a lack of coordinated institutional response mechanisms (Kimani & Wanjiru, 2023; Sewanyana & Okello, 2021). Furthermore, there is limited empirical evidence in Kenya assessing how these factors, namely perceived cyber risks, legal frameworks, and ethical practices, collectively influence the effectiveness of healthcare cybersecurity systems.

The absence of context-specific, evidence-based cybersecurity frameworks for public health institutions poses a critical risk to data security and patient trust. Without a clear understanding of the current threat landscape and the institutional readiness to mitigate such risks, healthcare systems may remain exposed to operational disruptions, data loss, and reputational damage. This study, therefore, sought to address this gap by examining the interplay between cyber threats, the Kenya Cybercrime Act, ethical data protection practices, and the cybersecurity framework at KNH, and to propose a contextually relevant model for strengthening cybersecurity in Kenya's healthcare sector.

1.2 Purpose of the Study

To examine the data protection ethical guidelines adopted by Kenyatta National Hospital to protect its healthcare system.

1.3 Research Questions

To what extent are data protection ethical guidelines adopted by Kenyatta National Hospital effective in mitigating healthcare cyber risks?

2. Literature Review

2.1 Theoretical Review

STS theory emerged from organizational research in the 1950s (Trist & Bamforth, 1951) to challenge the notion that technology alone determines system effectiveness. It emphasizes the interdependence between social factors (people, culture, processes) and technical components (tools, systems, infrastructure) (Pasmore et al., 1982). In cybersecurity, STS theory positions threats as socio-technical problems, where failures often arise from misalignment between technology and human or organizational elements (Malatji et al., 2019; Baxter & Sommerville, 2011). Regarding data protection, ethical guidelines adopted by KNH, STS theory underscores the importance of aligning technical safeguards with ethical standards and staff adherence. The theory suggests that effective data protection results from embedding ethical principles within both technical controls and social behaviors, including training, awareness, and organizational culture.

2.2 Empirical Review

The implementation of data protection ethical guidelines within healthcare institutions such as Kenyatta National Hospital (KNH) reflects the critical intersection between patient rights, institutional accountability, and digital security. Ethical data protection extends beyond

compliance with statutory mandates like the Kenya Data Protection Act (DPA, 2019); it encompasses informed consent, confidentiality, transparency, accountability, and patient autonomy. The literature reveals that while the ethical imperative is clearly articulated in policy frameworks, empirical evidence on its institutionalization, particularly in high-volume, resource-stretched hospitals like KNH, is still limited.

Globally, ethical data governance in healthcare has increasingly emphasized the role of informed consent as a foundation for patient autonomy and trust. Studies from developed health systems (Bărcanescu, 2021; Vayena & Blasimme, 2018) indicate that robust consent processes enhance both trust and treatment outcomes by empowering patients with knowledge and agency. In Kenya, the DPA aligns with these principles by mandating clear, informed, and revocable consent mechanisms (Nyaga et al., 2023). However, in the context of KNH, the implementation of these consent protocols has not been empirically documented. Mugo and Nzuki (2014), in a survey of EHR adoption in Kenyan hospitals, found that healthcare professionals often obtain consent as a formality, with little emphasis on patient understanding. This disconnects between ethical ideals and clinical practice, especially in tertiary care centers, raises concerns about the depth of patient agency in data governance. Comparable studies in Uganda and South Africa report similar superficial consent practices in public hospitals (Makulilo & Boshe, 2016; Dzenowagis et al., 2018), suggesting a regional implementation gap that warrants empirical exploration at KNH.

The principle of data minimization, collecting only necessary data for specific purposes, serves to mitigate the risks of unauthorized access and misuse. Although embedded in Kenya's DPA and emphasized in ethical codes (Omondi, 2023), evidence suggests that this guideline is inconsistently enforced. In Nigeria, Adebayo et al. (2021) found that health institutions frequently over-collect data without a clear rationale, increasing exposure to breaches. Similar findings are echoed by Abdullah et al. (2020) in East Africa, where poor digitization policies lead to redundant data capture. At KNH, which interfaces with insurance databases, international research bodies, and public health agencies, the challenge is compounded by multi-stakeholder access to patient data. Yet, studies evaluating whether KNH has internal guidelines limiting over-collection, or how such guidelines are enforced across departments, remain absent. This institutional gap underscores the need for research examining how ethical data minimization is operationalized in complex, multi-role public hospitals.

Confidentiality and data security are at the heart of ethical healthcare, especially in relation to sensitive medical information such as mental health, HIV status, or sexual and reproductive health. Globally, literature emphasizes that ethical data protection must include not only technical safeguards (encryption, access control) but also cultural competence and discretion in information sharing (Cohen et al., 2020; Choi et al., 2019). In Kenya, the KE-CIRT/CC and the CMCA establish national-level structures to prevent data breaches (Ouma, 2021), but institution-specific measures remain under-examined. At KNH, confidentiality breaches can have severe consequences given its role in treating vulnerable and marginalized populations. Research by Weerasinghe et al. (2020) shows that patients who fear confidentiality breaches may withhold information, undermining clinical outcomes. Despite the critical nature of this issue, there is a dearth of published case studies assessing breach frequency, staff practices, or IT vulnerability audits at KNH. Similar evaluations from India and South Africa, such as those by Singh et al. (2018), illustrate that where breach logs are systematically reviewed, confidentiality improves, offering a comparative gap for local inquiry.

Transparency and accountability are equally emphasized as ethical pillars in healthcare data governance. Literature from the EU and Canada (Kluge et al., 2021; Flahault, 2019) illustrates that clear communication about data use fosters trust and reduces resistance to digital record systems. Kenya's DPA obligates institutions to notify patients of breaches and explain data use policies, yet Omondi (2023) notes that public institutions often lack internal mechanisms to fulfill this obligation meaningfully. At KNH, there is no publicly available data on whether patients are routinely informed about how their health data is stored, shared, or potentially used for research. The absence of hospital-wide transparency metrics or routine ethics audits at KNH stands in contrast to models in Brazil and Estonia, where such audits are central to ethical compliance (de Freitas et al., 2022; Tikk & Kaska, 2020). This underscores the need for localized studies investigating whether KNH communicates its data practices clearly to patients, and how such practices vary across departments.

The right to data access, rectification, and erasure is another ethical dimension with strong international precedent. According to Vayena et al. (2018), patient access to personal records improves engagement and error correction in care processes. Kenya's DPA guarantees this right, but implementation remains fragmented. In a study of patient access in Nairobi County, Muthoni and Waweru (2020) found that many hospitals lacked platforms for patients to review their records, with some still using paper-based systems that were inaccessible to patients. The situation at KNH remains unclear, with little literature indicating whether patient portals or complaint redress systems exist to handle data correction or deletion requests. Comparative systems in South Korea and the UK have implemented electronic dashboards for this purpose (Kim & Park, 2019), suggesting that KNH could benefit from similar models. The research gap here is clear: there is little to no empirical evidence on how patient data access rights are being respected or enabled at KNH.

Continuous staff training is widely regarded as essential to translating ethical data protection principles into institutional culture. Literature from Asia and North America shows that SETA (Security Education, Training, and Awareness) programs improve compliance, reduce data mishandling, and increase ethical sensitivity among staff (Reeves et al., 2021; Tolossa, 2023). Kenyan studies indicate that training is often sporadic and focuses more on clinical than digital ethics (Mugo & Nzuki, 2014). While KNH, as a teaching hospital, may have more structured training opportunities, there is no available research evaluating the content, frequency, or ethical orientation of its staff education programs. In contrast, Singapore's public hospitals implement quarterly ethics modules specifically on digital privacy (Tan et al., 2020), pointing to a possible model for KNH. This suggests a significant gap in documentation and assessment of how ethics training is institutionalized in Kenya's largest hospital.

Lastly, patient empowerment and data literacy are frequently under-emphasized in both policy and practice. Empowered patients are more likely to engage in shared decision-making and demand accountability in data handling (Mittelstadt, 2017). Studies from Tanzania and Malawi (Zimba et al., 2021; Ngwira, 2018) show that when patients are informed of their data rights, they ask more critical questions and identify potential abuses. In Kenya, however, patient education on data rights is not widely integrated into routine care. At KNH, where patient literacy levels vary, the challenge of empowering users is heightened. There is a need to examine whether patient-facing communication, verbal, written, or digital, includes ethical data protection messaging. Without this, the legal guarantees of the DPA may remain inaccessible in practice.

The implications of examining this objective extend into both institutional reform and policy enhancement. First, identifying gaps in KNH's application of ethical data protection practices could inform the development of standardized protocols tailored for high-volume public hospitals. As Omondi (2023) emphasizes, ethical data governance is only effective when embedded into everyday clinical operations. A systematic evaluation of KNH's practices could therefore serve as a national benchmark for other referral facilities, particularly in contexts where digital health systems are rapidly expanding. Moreover, such an examination supports Kenya's broader digital health strategy, which aspires to integrate data protection into national e-health platforms (Ministry of Health, Kenya, 2021).

At an operational level, insights from this objective may inform capacity-building priorities. For example, if gaps in staff training are identified, KNH could design modular ethics workshops modeled after global best practices (Tan et al., 2020). Similarly, if patient consent processes are found to be inadequate, hospital administrators may re-engineer intake workflows to enhance transparency. These improvements are not merely regulatory; they directly affect health outcomes, patient satisfaction, and institutional trust (Weerasinghe et al., 2020).

Nonetheless, KNH faces distinct challenges in implementing ethical data protection. As a tertiary and teaching hospital with national referral obligations, its departments are diverse, high-pressure, and resource-constrained. According to Mugo & Nzuki (2014), such institutional scale often leads to fragmented implementation of IT policies, with some departments far more compliant than others. Furthermore, reliance on donor-funded systems or third-party software common in many public institutions introduces ethical complexity around data ownership and third-party access (Makulilo & Boshe, 2016; Singh et al., 2018). The heterogeneity of digital maturity across KNH's departments further complicates the establishment of centralized, enforceable ethical standards.

Additionally, KNH's role in medical education presents both an opportunity and a risk. While it could serve as a hub for ethical data protection training, the transient nature of medical interns and students may dilute long-term accountability unless ethical instruction is deeply embedded into academic curricula (Reeves et al., 2021). Lastly, the absence of transparency reports, public disclosures of breaches, or audit summaries at KNH makes it difficult to assess whether accountability mechanisms are functioning effectively. In summary, this objective not only fills a pressing research void but also carries practical significance for institutional resilience, regulatory compliance, and patient rights. Its findings could help transform KNH from a passive implementer of ethical guidelines to an active model of data protection governance within the region.

3. Methodology

This study adopted a descriptive research design to examine cybersecurity threats and countermeasures within the healthcare sector, focusing specifically on Kenyatta National Hospital (KNH). The target population includes all staff categories involved in patient care, information management, and IT infrastructure (Clinical staff, ICT department, and Health records and admins) as they are integral to cybersecurity issues in the hospital setting. The accessible population consisted of 5,983 staff who were available and consented to participate in the study during the data collection period. A stratified random sampling technique was deemed the most appropriate. It involves dividing the population into distinct, non-overlapping

strata based on shared characteristics such as job roles or departments. Within each stratum, simple random sampling was used to select participants. The sample size of 370 was determined based on a population of 4,933 staff members relevant to the study (clinical staffs, ICT, and health records and admin staffs) out of an approximate total population of 5,983(total staffs at KNH), using a 95% confidence level and a 5% margin of error, following the Yamane (1968) sample size formula. A pilot study was conducted at Mbagathi Hospital to pretest the research instruments, ensuring that the questionnaire items effectively capture the intended information and identify any ambiguities or inconsistencies. In this study, internal validity was enhanced through consistent administration of the data collection instruments, controlling environmental variables by surveying all respondents within the same hospital setting, and employing a pilot study to refine the tools. External validity is supported by the use of stratified sampling and selecting a sample representative of Kenyatta National Hospital's diverse staff, improving the applicability of findings to similar healthcare institutions in Kenya.

4. Results and Discussion

4.1 Reliability Statistics

In this study, the Cronbach's alpha for the questionnaire was 0.691 across four items. Although slightly below the ideal 0.7 threshold, this value is acceptable for preliminary studies and exploratory research, suggesting adequate internal consistency. This supports the reliability of the instrument while acknowledging a minor limitation in the precision of measurement.

Table 1: Reliability Statistics

Cronbach's Alpha	N of Items
.691	4

4.2 Response Rate

The research issued a total of 370 questionnaires, out of which 365 were filled and returned, giving a response rate of 94.8%. According to Mugenda and Mugenda (2002), a sample size of 30% and above was considered sufficient for the study; hence, the 94.8% response rate was considered sufficient, as presented in Table 2.

Table 1: Response Rate

Variable	Frequency	Percentage %
Filled and returned	365	98.65
Non-response	5	1.35
Total	**370**	**100**

4.3 Examine data protection ethical guidelines on Healthcare Cybersecurity risks at KNH.

The study examined the data protection ethical guidelines implemented at Kenyatta National Hospital and their role in mitigating healthcare cybersecurity risks. The results are presented in Table 3.

Table 3: Descriptive analysis on the Influence of Data Protection Ethical Guidelines on Healthcare Cybersecurity risks at KNH

	N	Mean	Std Dev	Var
KNH has a documented code of ethics that defines how patient data should be accessed, stored, shared, and protected to ensure responsible use.	365	3.83	1.166	1.359
KNH provides regular training to staff on ethical standards for handling patient information, including issues like confidentiality, informed consent, and professional conduct.	365	3.98	1.182	1.398
KNH implements the principles of confidentiality, integrity, and availability by using secure login systems, restricted access to sensitive files, and reliable data backup procedures.	365	4.01	1.193	1.423
KNH takes disciplinary action when ethical violations occur, such as unauthorized access to medical records, negligent disclosure of private data, or mishandling of patient files.	365	3.97	1.176	1.384
Patients at KNH are informed about how their personal health data is handled, including who can access it, the purposes for data use, and their rights under ethical and legal guidelines.	365	3.93	1.152	1.328
Total Avg	**365**	**3.94**	**1.17**	**1.38**

The findings in Table 3 related to data protection ethical guidelines at Kenyatta National Hospital (KNH) demonstrate a strong institutional emphasis on ethical behaviour in safeguarding patient information. Among the examined items, the highest-rated practice was the implementation of the principles of confidentiality, integrity, and availability through mechanisms such as secure login systems, restricted access to sensitive data, and regular data backups. This item received a mean score of 4.01 (SD = 1.19), suggesting widespread agreement among respondents that KNH prioritizes ethical control of digital information. This practice aligns with the Socio-Technical Systems (STS) Theory, which posits that robust cybersecurity requires alignment between technological safeguards and ethical human behaviour. These technical-environmental controls are supported by routine training and institutional policy enforcement, thus enabling the ethical dimension of data protection to be

realized within a working system. The implementation of these principles mirrors observations by Lee & Smith (2023), who asserted that system design and ethical culture must be integrated to ensure resilience in data handling. Roberts and Anderson (2023) similarly observed that confidentiality and role-based access controls significantly reduce data exposure risks in hospital networks. Zhou and Tang (2021) emphasized that technical ethics mechanisms, such as authentication and redundancy, ensure compliance and mitigate human error, a concept evident in the practices at KNH.

Closely following this was the finding that KNH provides regular training to staff on ethical standards, which achieved a mean score of 3.98 (SD = 1.18). This indicates that hospital personnel are periodically educated on key ethical issues, including confidentiality, informed consent, and professional data handling. The relevance of this finding is best interpreted through the lens of Institutional Theory, which emphasizes that formal rules, norms, and values are embedded within organizations to enhance legitimacy and compliance. Training is a vital normative tool through which ethical standards are institutionalized, making them an expected and shared part of organizational behaviour. Studies by Johnson & Becker (2022) highlight how recurring training fosters ethical commitment and reduces internal violations. Alahmari et al. (2023) further argued that ethical training helps transform awareness into embedded behaviour, especially in clinical settings where information flows rapidly. In the Kenyan context, such efforts are critical for aligning healthcare practice with both national policy and international privacy standards, reinforcing the importance of institutionalized ethics.

Another significant finding was that KNH enforces disciplinary action for ethical violations, such as unauthorized access to records or negligent disclosure of patient information. This item scored 3.97 (SD = 1.18), demonstrating strong agreement that there are consequences for unethical conduct. This is clearly aligned with Deterrence Theory, which posits that the presence of credible sanctions discourages individuals from engaging in violations. When staff are aware that ethical breaches have tangible repercussions, their likelihood of engaging in such behaviour diminishes. This is particularly important in high-risk environments like hospitals, where data sensitivity is paramount. Supporting this interpretation, Martin & Williams (2022) found that ethical misconduct in healthcare organizations declined when clear punitive structures were in place. Similarly, Perakslis (2014) emphasized that deterrent mechanisms must be consistently enforced to support a sustainable culture of privacy and accountability.

The finding that patients are informed of how their data is handled, with a mean of 3.93 (SD = 1.15), indicates the hospital's effort to promote transparency and informed consent, which are key pillars of ethical data management. This again resonates with Institutional Theory, which emphasizes that ethical legitimacy is shaped by external expectations, including patient rights and legal mandates. Informing patients of how their data is used and who can access it not only meets legal obligations but also strengthens the ethical relationship between healthcare providers and service users. Literature supports this approach: Kumar & Singh (2023) found that patients are more cooperative and satisfied with care when their rights are acknowledged and protected. Smith & Jones (2020) also noted that hospitals with strong patient communication protocols reported fewer complaints and higher levels of trust in digital systems.

The lowest-scoring item among the examined ethical practices was the existence of a documented code of ethics governing access, storage, and sharing of patient data, with a mean

score of 3.83 (SD = 1.17). While still reflecting general agreement, this result suggests some variability in staff awareness or understanding of the code. From a Socio-Technical Systems perspective, the presence of an ethical code must be complemented by technological tools and clear dissemination strategies. A code of ethics that exists only in documentation, without integration into workflows and systems, may fail to produce the intended behavioural outcomes. Research by Almutairi et al. (2020) affirms this by showing that ethical guidelines are most effective when combined with digital policies and technical restrictions. Meanwhile, Elshenawy et al. (2021) argue that codes of conduct become operationally meaningful only when they are embedded within user interfaces, data access routines, and staff performance reviews. Thus, although KNH has taken steps to establish ethical norms, greater clarity, visibility, and integration of these norms across hospital systems would enhance their effectiveness.

These descriptive findings are strongly supported by inferential statistics. Regression analysis identified data protection ethical guidelines as the strongest predictor of the cybersecurity framework at KNH, with a standardized coefficient (β) of 0.309 and an unstandardized coefficient B = 0.303 ($p < 0.001$). This statistically significant positive relationship confirms that stronger ethical controls and practices directly improve the hospital's cybersecurity posture. The result validates the theoretical premise of the Socio-Technical Systems Theory, which holds that security is most effective when organizational ethics and technical safeguards co-evolve. In the same regression model, data protection ethics outperformed both legal and risk variables in explaining variance in the cybersecurity framework, highlighting its critical influence.

The correlation analysis further supported this relationship, showing a moderate and statistically significant association ($r = 0.294$, $p < 0.01$) between ethical guidelines and the cybersecurity framework. This suggests that as ethical standards become more embedded, confidence in KNH's cybersecurity systems also improves. This relationship reflects both Institutional and STS perspectives, as ethical standards, when formally established and practically implemented, become institutionalized and positively affect user behaviour and system performance.

Taken together, these results affirm that ethical data protection practices at KNH are a cornerstone of its cybersecurity efforts. Ethical guidelines are not only recognized by staff but also actively shape behaviour, influence technical configuration, and improve institutional trust in cybersecurity mechanisms. As the strongest predictor in the study, they form a critical foundation for building resilient, trustworthy, and effective digital healthcare systems.

4.4 Summary of the findings

The findings provide a comprehensive analysis of ethical practices related to patient data management at Kenyatta National Hospital (KNH). Across the five key items assessed, the overall mean is 3.94, with a standard deviation of 1.17 and a variance of 1.38. These results indicate a general agreement among respondents that KNH upholds ethical standards in managing patient information, with moderate variability suggesting some differences in perceptions regarding the consistency and effectiveness of these practices. The item "KNH has a documented code of ethics that defines how patient data should be accessed, stored, shared, and protected to ensure responsible use" recorded a mean score of 3.83 (SD 1.17, Var 1.36). This reflects agreement that a formal ethical framework exists to guide responsible data

management, although the moderate variability points to some differences in how clearly this code is understood or implemented across the hospital. The provision of regular staff training on ethical standards for handling patient information, including confidentiality, informed consent, and professional conduct, received a mean score of 3.98 (SD 1.18, Var 1.40). This suggests strong agreement that KNH actively supports staff through training, reinforcing ethical responsibilities, though the variability indicates differing views on the sufficiency or frequency of such training. The item addressing the implementation of confidentiality, integrity, and availability principles through secure login systems, restricted access, and reliable data backup procedures scored the highest mean of 4.01 (SD 1.19, Var 1.42). This denotes widespread acknowledgment that KNH operationalizes these core ethical principles effectively, yet the moderate variability suggests some respondents perceive inconsistencies in technical or procedural safeguards. Regarding accountability, the statement "KNH takes disciplinary action when ethical violations occur, such as unauthorized access to medical records, negligent disclosure of private data, or mishandling of patient files" achieved a mean of 3.97 (SD 1.18, Var 1.38). This indicates agreement that mechanisms exist to address ethical breaches, with some variation in perceptions of how consistently or rigorously such measures are applied. Lastly, the item "Patients at KNH are informed about how their personal health data is handled, including who can access it, the purposes for data use, and their rights under ethical and legal guidelines" scored a mean of 3.93 (SD 1.15, Var 1.33). This reflects general agreement that patient communication regarding data handling is a priority, though the variability suggests that this communication may not be uniformly experienced or fully understood by all patients.

5. Conclusion

With respect to data protection ethical guidelines, the study found that they were the most influential predictor of the strength of the cybersecurity framework. Staff agreed that ethical principles such as confidentiality, integrity, and accountability were well understood and partially enforced. Regular training and disciplinary measures were also in place, albeit inconsistently. The conclusion drawn is that ethical norms play a foundational role in sustaining secure digital environments in healthcare. When these guidelines are well-communicated and embedded in practice, they promote responsible system use and help bridge gaps left by technological or legal limitations. Thus, a values-driven approach to cybersecurity is critical for institutional resilience.

Finally, the study proposed a framework for establishing effective cybersecurity in the healthcare sector, informed by the evaluation of KNH's practices. The analysis of five operational areas-simulation preparedness, training, resource allocation, policy enforcement, and incident response revealed moderate levels of maturity, with simulation drills being the most developed and incident response the weakest. The conclusion is that cybersecurity at KNH, and similar public healthcare institutions, requires a more integrated and structured model. This model should align leadership, policy, training, and technology under a unified strategy grounded in Socio-Technical Systems (STS) Theory. Such an approach ensures that both human and technical factors work in synergy to protect patient data and institutional integrity.

6. Recommendations and Contributions of the Study

Ethical data protection guidelines were identified as the strongest predictor of an effective cybersecurity framework. However, inconsistencies in training and partial enforcement were noted. The study recommends that KNH should institutionalize ethical guidelines by embedding them into everyday workflows, onboarding protocols, and performance appraisals. Comprehensive, role-specific training should be offered consistently across all departments. Furthermore, the management should develop an e-learning module on healthcare data ethics, tailored to job functions (e.g., clinicians, IT staff, administrative personnel), and make certification mandatory on an annual basis.

References

Abdullah, R., Hamid, N. A. A., & Jaber, M. M. (2020). Cybersecurity in healthcare: A systematic review of modern threats and solutions. *Health Informatics Journal*, *26*(2), 981–1000.

Adebayo, A. M., Olamijulo, J. A., & Fapohunda, T. M. (2021). Ethical issues in health information management in Nigeria. *Nigerian Journal of Health Sciences*, *21*(1), 34–41.

Alahmari, S., Alghamdi, A., & Khalid, A. (2023). Integrating ethical awareness and cybersecurity practices among healthcare employees: A training-based study. *Journal of Medical Systems, 47*(2), 25.

Almutairi, M., Sarfraz, M., & Siddiqui, M. (2020). Insider threat mitigation in healthcare environments: A review of practices and policy gaps. *International Journal of Information Management, 50*(1), 228–235.

Barcanescu, E. D. (2021). Informed consent in the digital age: Legal and ethical dimensions in medical data protection. *Journal of Medical Ethics and History of Medicine*, *14*(1), 22–31.

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers, 23*(1), 4–17.

Beauchamp, T. L., & Childress, J. F. (2019). *Principles of Biomedical Ethics* (8th Ed.). Oxford University Press.

Choi, Y., Park, J., & Kim, H. (2019). Ethical management of patient data in digital healthcare: Global practices and local implications. *International Journal of Medical Informatics*, *129*(1), 132–138.

CIPIT. (2021). *Healthcare data governance in Kenya: Challenges and Recommendations*. Centre for IP and IT Law, Strathmore University.

Cohen, I. G., Amarasingham, R., Shah, A., Xie, B., & Lo, B. (2020). The legal and ethical concerns that arise from using complex predictive analytics in health care. *Health Affairs*, *39*(5), 783–791.

Dzenowagis, J., Seedhouse, D., & Schicktanz, S. (2018). Patient consent in sub-Saharan healthcare systems: A literature review. *Developing World Bioethics*, *18*(3), 189–200.

Elshenawy, N., Hasan, M., & Alharby, M. (2021). Legal and institutional determinants of cybersecurity policy implementation in healthcare organizations. *Information & Computer Security, 29*(2), 287–303.

Flahault, A. (2019). Transparency in health data governance: The Canadian perspective. *Canadian Journal of Public Health*, *110*(2), 128–131.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2022). A retrospective impact analysis of cyberattacks on UK hospital IT systems. *BMJ Health & Care Informatics, 29*(1), e100501.

Johnson, D., & Becker, A. (2022). Ethics in health IT: The role of training in reducing privacy violations. *Journal of Health Ethics, 18*(1), 48–61.

Kenya Law. (2019). *The Data Protection Act No. 24 of 2019*. National Council for Law Reporting.

Kenyatta National Hospital (KNH) (2018). *Strategic plan (2018-2023).* https://knh.or.ke/wp-content/uploads/2022/01/KNH_Strategic_Plan-2018-2023_FINAL.pdf

Kim, S., & Park, J. (2023). Dynamic capabilities for cybersecurity resilience: A multi-level approach. *Information Systems Research, 34*(2), 453-471.

Kimani, D., & Wanjiru, R. (2023). Cybersecurity investment gaps in Kenyan public hospitals: A call for strategic alignment. *African Journal of Health Systems, 18*(2), 76–89.

Kluge, E. H., Gøeg, K. R., & Moen, A. (2021). Ethical dimensions of digital health systems in Europe: A review of the literature. *International Journal of Medical Informatics*, 150, 104451.

Kumar, N., & Singh, A. (2023). *Ethical data governance in public healthcare: Enhancing patient trust through transparency*. BMC Medical Ethics, 24(1), 11.

Lee, Y., & Smith, K. (2023). Socio-technical approaches to digital health resilience: Ethics, usability, and interoperability. *International Journal of Medical Informatics, 170*(1) 104981.

Maher, B., & Kruger, H. A. (2022). Ethical risks in digital health: A review of emerging threats. *Health Technology and Society*, *15*(2), 91–106.

Makulilo, A. B., & Boshe, P. (2016). The efficacy of data protection laws in East Africa: Comparative insights. *African Human Rights Law Journal*, 16(2), 353–375.

Malatji, E., Flowerday, S., & Sibiya, G. (2019). A socio-technical approach to information security management. *South African Journal of Information Management, 21*(1), 1–10.

Martin, L. J., & Williams, T. A. (2022). *The effects of ethical enforcement on healthcare staff behavior: Evidence from disciplinary records*. Journal of Health Administration, 56(3), 211–224.

Ministry of Health, Kenya. (2021). *Kenya National eHealth Policy 2021–2030*. Government of Kenya. https://www.health.go.ke

Mittelstadt, B. D., & Floridi, L. (2016). The ethics of big data in health. *Philosophy & Technology*, 29(4), 331–341.

Mugo, D. M., & Nzuki, D. M. (2014). Determinants of electronic health record adoption among hospitals in Kenya. *International Journal of Information and Communication Technology Research*, *4*(4), 116–123.

Muthoni, M. G., & Waweru, M. K. (2020). Patient access to health records and institutional compliance in Nairobi public hospitals. *East African Medical Journal*, *97*(8), 412–418.

Mutinda, K., & Ongus, R. (2020). An assessment of cybersecurity frameworks in public hospitals in Kenya. *International Journal of Scientific and Research Publications, 10*(8), 476–482.

Ngwira, A. (2018). Raising patient awareness of health data rights in Malawi: A qualitative study. *Malawi Medical Journal*, *30*(3), 220–224.

Nyaga, R., Ondego, J., & Joel, K. (2023). Data protection and healthcare privacy in Kenya: Evaluating the Data Protection Act. *African Journal of ICT Policy and Practice*, *11*(1), 55–72.

Office of the Data Protection Commissioner. (2022). *Annual report on data protection in Kenya*. Nairobi: ODPC.

Omondi, C. (2023). Ethical considerations in handling patient health data in Kenya. *Bioethics & Health Law Review*, *2*(1), 45–60.

Ouma, C. (2021). KE-CIRT/CC's role in national cybersecurity resilience. *Kenya Cybersecurity Journal*, *3*(2), 19–29.

Perakslis, E. D. (2014). Cybersecurity in health care: A story of data integrity, patient safety, and regulatory compliance. *Therapeutic Innovation & Regulatory Science, 48*(5), 589–595.

Reeves, S. L., Calic, D., & Delfabbro, P. (2021). Cybersecurity training effectiveness: A meta-analysis of SETA programs. *Journal of Cybersecurity Education, Research and Practice*, *5*(1), 4.

Sewanyana, J., & Okello, D. (2021). Cybersecurity policy implementation and institutional preparedness in East Africa: A healthcare sector perspective. *East African Journal of Information and Communication, 2*(1), 43–58.

Shachar, C., Engel, J., & Elwyn, G. (2020). Digital health and the ethics of data use. *JAMA*, *323*(5), 507–508.

Singh, S., Sharma, P., & Agarwal, S. (2018). Data governance and cybersecurity resilience in healthcare organizations. *Health Services Management Research*, *31*(2), 70–79.

Tan, T. B., Wong, J. Y., & Koh, G. C. H. (2020). Integrating data ethics into digital health training: Lessons from Singapore. *Asia Pacific Journal of Public Health*, *32*(6–7), 301–307.

Tikk, E., & Kaska, K. (2020). The Estonian model for data security and transparency in e-health systems. *Journal of Cyber Policy*, *5*(1), 92–109.

Tolossa, B. (2023). Phishing in healthcare: Emerging trends and prevention in African hospitals. *Journal of African Health Informatics*, *9*(1), 44-55.

Vayena, E., & Blasimme, A. (2018). Health data ethics in the age of big data. *Nature Medicine*, *24*(5), 462–464.

Weerasinghe, I. M. S., Sivarajah, U., & Irani, Z. (2020). Improving healthcare outcomes through information security: Patient trust as a critical factor. *Health Informatics Journal*, *26*(1), 434–448.

Willis, J. (2015). The politics of hospital care in Kenya: Case of Kenyatta National Hospital. *African Affairs, 114*(456), 578–600.

Yamane, T. (1967) Statistics: An introductory analysis (2nd Ed.). Harper and Row, New York.

Zhou, X., & Tang, L. (2021). Technical ethics in hospital data governance: Automation, risk, and accountability. *Journal of Information Ethics, 30*(2), 49–66.

Zimba, R., Banda, R., & Kayuni, H. (2021). Educating patients on data rights in rural Tanzania: An intervention study. *African Journal of Public Health*, *15*(2), 112–120.