



**International Journal of
Strategic Management, Accounting *and*
Human Resources Management**

Peer-Reviewed Academic Journal



Volume 1 | Issue No.5 | 2026 | ISSN: 1234-5678

Chief Editor: Prof. John A. Orodho

Managing Editor: Dr. James O. Oringo

Executive Editor: Mr. David W. Ngigi

Associate Editor: Dr. Jakline Benjamin Libo

Editorial Board:

Chairman: Prof. George Orwa

Dr. Saad Okwiri

Dr. Mohammed Hussain Yousif Izzeddin

Dr. Henry Kegoro

IJSAHM Publications

www.ijсахm.org

RISK-BASED GOVERNANCE AND AUDIT FRAMEWORK FOR ARTIFICIAL INTELLIGENCE IN KENYA'S HEALTHCARE SECTOR

A comprehensive reference report for promoting the safe, ethical, transparent, accountable and trustworthy use of Artificial Intelligence in Kenya's healthcare sector.

Dr. James Odhiambo Oringo

A Post Doctorate Fellow on AI Ethics and Governance in Africa at the Policy Innovation Centre and African Hub for Innovation and Development, in Nigeria.

Abstract

This capstone study was undertaken at the end of a fellowship on AI Ethics and Governance in Africa Organized by the Policy Innovation Centre and African Hub for Innovation and Development, in Nigeria. Artificial Intelligence (AI) is increasingly becoming part of healthcare transformation in Kenya, with applications spanning diagnostic support, disease surveillance, telemedicine, health information management, predictive analytics and administrative decision support. The study responds to a governance gap: Kenya has developed an important legal and policy foundation for digital health and AI, but the existing arrangements do not yet constitute a single, operational, risk-based healthcare AI governance and audit system. The capstone adopted a desk-based qualitative design supported by systematic literature review and document analysis. Evidence was drawn from peer-reviewed literature, Kenyan legislation and policy documents, international standards, AI governance frameworks and reports from authoritative organizations. Priority was given to literature published between 2020 and 2026, while seminal sources were retained where they provided foundational theoretical or conceptual value. The findings show that AI adoption is progressing, but institutional readiness is uneven. National referral hospitals, research institutions, private facilities and donor-supported programmes are relatively more active, while county and primary healthcare settings face greater infrastructure, skills, financial, data, interoperability and governance constraints. The study further found that Kenya's Kenya National Artificial Intelligence Strategy 2025–2030, Digital Health Act 2023 and Data Protection Act 2019 provide an important foundation, but significant AI-specific gaps remain around risk classification, algorithmic accountability, explainability, independent auditing, post-deployment monitoring, lifecycle governance and liability. Five interrelated categories of risk were identified: governance, ethical, technical, operational and regulatory. The study found that these risks interact and cannot be managed effectively through isolated controls. International frameworks reviewed, WHO, OECD, the EU AI Act, NIST AI RMF and ISO/IEC 42001, offer complementary strengths, but none can be transferred to Kenya unchanged. The principal deliverable is therefore a context-specific Risk-Based Governance and Audit Framework. The framework combines governance leadership, legal and ethical compliance, risk assessment and classification, lifecycle governance, human and clinical oversight, continuous monitoring, independent AI auditing and continuous learning. It adopts a proportional approach in which higher-risk healthcare AI receives more rigorous validation, monitoring and independent assurance. The report concludes that responsible AI adoption in Kenya requires a shift from principle-based statements alone towards operational governance. The proposed framework provides a practical reference for policymakers, regulators, healthcare institutions, professionals, AI developers, auditors, researchers and other stakeholders seeking to promote safe, ethical, transparent, accountable and trustworthy AI in healthcare.

Key Words: Risk-Based Governance; Audit Framework; Artificial Intelligence; Healthcare Sector

1. INTRODUCTION

1.1 Artificial Intelligence in Healthcare

Artificial Intelligence refers to computer systems capable of performing tasks associated with human intelligence, including learning from data, pattern recognition, prediction, problem solving and decision support. In healthcare, advances in machine learning, deep learning, natural language processing and computer vision have expanded the range of AI applications. These include diagnosis, medical imaging, disease prediction, patient monitoring, precision medicine, drug discovery, clinical decision support and healthcare administration (Bouderhem, 2024; World Health Organization, 2021). The potential value of AI is considerable. AI can process large volumes of information rapidly, support clinicians with evidence-based insights, improve workflow efficiency, strengthen surveillance and help allocate scarce resources. However, healthcare is a high-impact environment. An inaccurate, biased, poorly validated or insecure AI system can contribute to patient harm, privacy violations, discrimination, clinical error and loss of public trust. The governance question is therefore not whether AI should be used, but under what conditions it can be used responsibly.

1.2 AI Governance and the Need for a Risk-Based Approach

AI governance comprises the rules, institutional structures, processes and technical mechanisms used to ensure that AI systems are designed, developed, deployed and monitored in accordance with

legal requirements, ethical values, organizational objectives and societal expectations (Mäntymäki et al., 2022). In healthcare, governance must extend beyond ordinary regulatory compliance to include patient safety, clinical accountability, data stewardship, human oversight and management of AI-related harms.

A risk-based approach recognizes that AI applications do not create identical levels of risk. Governance obligations should therefore be proportionate to potential harm. Systems that can materially influence diagnosis, treatment, triage, clinical prioritization or access to essential care require more rigorous assessment and assurance than low-impact administrative automation. This principle is consistent with the risk-based approaches reflected in the OECD and EU AI Act and with lifecycle risk management in the NIST AI RMF.

1.3 Kenya's Healthcare AI Context

Kenya has established a strong foundation for digital transformation through the Kenya National Artificial Intelligence Strategy 2025–2030, the Digital Health Act 2023, the Data Protection Act 2019 and related digital-health instruments. The Kenya AI Strategy identifies healthcare as a priority sector for AI adoption. Despite these developments, the capstone literature found that AI governance in healthcare remains fragmented and that practical guidance on AI risk classification, auditing, post-deployment monitoring, transparency and accountability remains limited.

1.4 Problem Statement

The central problem addressed by the capstone is the gap between increasing AI adoption and the availability of integrated governance and audit mechanisms capable of managing the associated risks. Existing laws and policies provide important foundations, but they do not by themselves establish a comprehensive operational architecture for risk classification, AI lifecycle governance, independent auditing, continuous monitoring and clear accountability for AI-related harm. This creates uncertainty for healthcare institutions, regulators, professionals, patients and technology developers.

1.5 Purpose and Objectives

- The purpose of the capstone is to develop a Risk-Based Governance and Audit Framework for Artificial Intelligence in Kenya's healthcare sector that promotes safe, ethical, transparent, accountable and trustworthy AI adoption.
- Objective I: To examine the current landscape of Artificial Intelligence adoption within Kenya's healthcare sector.
- Objective II: To analyse the existing legal, policy, regulatory and institutional frameworks governing Artificial Intelligence in Kenya's healthcare sector.
- Objective III: To identify the governance, ethical, technical, operational and regulatory risks associated with the adoption of Artificial Intelligence in Kenya's healthcare sector.
- Objective IV: To carry out comparative analysis of international best practices and existing Artificial Intelligence governance and audit frameworks applicable to healthcare.
- Objective V: To develop a Risk-Based Governance and Audit Framework for Artificial Intelligence in Kenya's healthcare sector.

1.6 Scope

The capstone focuses on governance, legal, regulatory, ethical, organizational and technical dimensions of AI implementation in healthcare. It covers the AI lifecycle from design and procurement through validation, deployment, monitoring, auditing, updating and retirement. It does not test the technical performance of individual algorithms, develop AI software or evaluate a specific clinical AI product.

2. METHODOLOGY

2.1 Research Design

The capstone adopted a desk-based qualitative research design supported by systematic literature review and document analysis. The design was appropriate because the purpose was to synthesize existing knowledge and governance evidence rather than collect primary data from human participants.

2.2 Sources of Evidence

Evidence was obtained from peer-reviewed journal articles, books, Kenyan legislation and policy documents, international standards, AI governance frameworks and reports from authoritative organizations including WHO, OECD, NIST, ISO, UNESCO and the European Union. Priority was given to literature published from 2020 to 2026, while seminal sources were retained where necessary.

2.3 Research Strategy

The study used electronic databases and scholarly platforms including Scopus, Web of Science, PubMed, Google Scholar, IEEE Xplore, SpringerLink and ScienceDirect. Search terms included Artificial Intelligence, AI governance, AI audit, AI risk management, healthcare AI, digital health, AI regulation, AI ethics, Kenya healthcare and AI governance framework. Boolean operators were used to improve retrieval precision.

2.4 Inclusion and Exclusion Criteria

Included evidence comprised peer-reviewed publications, official government documents, international standards, policy reports, AI

governance frameworks and English-language sources relevant to healthcare AI governance. Opinion pieces without empirical or policy evidence, duplicates, unrelated non-healthcare AI studies and publications lacking sufficient methodological rigor were excluded.

2.5 Data Analysis

The evidence was analysed thematically. Extracted material was coded and organized around AI adoption; legal and regulatory frameworks; governance and implementation risks; international best practices; AI governance frameworks; and governance and auditing requirements. The themes were then synthesized against the five capstone objectives. The resulting synthesis provided the design requirements for the proposed framework.

2.6 Framework Development

The proposed framework was developed by integrating the findings from the theoretical and empirical literature, international governance frameworks and Kenya's legal and institutional environment. The development process deliberately combined international principles with local context rather than importing an external framework unchanged.

2.7 Ethical Considerations

The capstone relied solely on publicly available secondary data and did not involve human participants or collection of personal information. Academic integrity was maintained through source attribution, appropriate citation and accurate representation of the reviewed evidence.

3. FINDINGS AND DISCUSSION

3.1 Current Landscape of AI Adoption

The review established that AI adoption in Kenya's healthcare sector is expanding, particularly in diagnostic imaging, disease surveillance, telemedicine, health information management, predictive analytics and administrative decision support. Adoption is more visible in national referral hospitals, research institutions, private facilities and donor-supported programmes, while county referral and primary healthcare facilities generally face greater implementation constraints. Institutional readiness varies because of differences in digital infrastructure, financial resources, workforce competencies, data quality, cybersecurity capacity and organizational governance. The findings therefore show that technology availability does not automatically translate into safe implementation. Governance capacity must develop alongside technological capacity.

The principal implication is that national AI adoption strategies should be accompanied by governance capacity-building, workforce development, infrastructure investment and mechanisms that prevent AI from reinforcing existing inequalities in healthcare access.

3.2 Legal, Policy, Regulatory and Institutional Frameworks

Kenya has an important governance foundation through the Kenya National Artificial Intelligence Strategy 2025–2030, Digital Health Act 2023 and Data Protection Act 2019. The Digital Health Act supports digital health governance, interoperability and secure management of health information, while the Data Protection Act provides safeguards for personal data, including sensitive health information.

The governance environment involves multiple institutions with complementary responsibilities, including the Ministry of Health, the Digital Health Agency, the Office of the Data Protection Commissioner and professional regulatory bodies. The review nevertheless identified fragmented AI-specific oversight. Existing instruments provide limited operational guidance on algorithmic accountability, explainability, AI certification, independent auditing, continuous monitoring, liability allocation and full lifecycle governance.

3.3 Governance, Ethical, Technical, Operational and Regulatory Risks

Governance risks include unclear accountability, fragmented oversight, inadequate governance committees and undefined decision-making responsibilities. Ethical risks include algorithmic bias, discrimination, limited explainability, privacy concerns, inadequate consent and threats to patient autonomy.

Technical risks include poor data quality, cybersecurity vulnerabilities, model drift, interoperability problems, algorithmic error and inadequate validation. Operational risks include limited financial resources, infrastructure constraints, skills shortages, resistance to change and weak institutional capacity. Regulatory risks include uncertainty over liability, certification, post-deployment surveillance, continuous compliance and independent audit requirements.

The central finding is that these risks are interconnected. A data-quality problem can become a clinical-safety problem; a governance weakness can become a legal or accountability problem; and a cybersecurity incident can become a patient-safety and public-trust problem. Risk management therefore needs to operate as an integrated system.

3.4 International Best Practices

The WHO framework provides healthcare-specific ethical principles including human autonomy, wellbeing, transparency, accountability, inclusiveness and equity. The OECD provides principles for trustworthy AI and risk-based policy. The EU AI Act provides a legally enforceable risk-based regulatory model. NIST AI RMF provides practical lifecycle risk-management functions, while ISO/IEC 42001 provides an auditable AI management-system approach. UNESCO and related international guidance reinforce human rights, fairness, human oversight and responsible innovation.

3.5 Comparative Synthesis

The comparison shows strong convergence around transparency, accountability, fairness, human oversight, privacy, safety, risk management and continuous improvement. The frameworks differ mainly in legal status, scope and implementation mechanisms. No single framework fully addresses Kenya's healthcare context. The appropriate approach is therefore a hybrid model combining WHO healthcare ethics, OECD principles, EU risk-based regulatory thinking, NIST lifecycle risk management and ISO/IEC 42001 management-system controls.

3.6 Requirements for the Proposed Framework

The findings establish eight interrelated requirements: governance leadership and institutional oversight; legal, ethical and regulatory compliance; AI risk assessment and classification; lifecycle governance; ethical and clinical oversight; continuous monitoring and performance management; independent AI auditing; and continuous learning and improvement. These requirements constitute the principal design basis of the framework presented in Section 4.

4. PROPOSED RISK-BASED GOVERNANCE AND AUDIT FRAMEWORK

4.1 Rationale

The proposed framework responds to the gap between increasing AI adoption and fragmented AI-specific governance. It is designed as a practical operational layer that complements Kenya's existing legal and policy environment. Its central proposition is that AI governance is a continuous institutional responsibility rather than a one-time approval exercise.

4.2 Guiding Principles

- Patient safety first.
- Human-centred decision-making and meaningful human oversight.
- Risk proportionality.

- Lawfulness and regulatory alignment.
- Transparency and explainability.
- Fairness and non-discrimination.
- Privacy and responsible data stewardship.
- Security and resilience.
- Lifecycle accountability.
- Independent assurance and continuous improvement.

4.3 Framework Architecture

The framework is layered and cyclical. The policy and regulatory layer establishes the mandate. Institutional governance provides accountability. Risk assessment determines the level of controls required. Lifecycle governance applies those controls from planning through retirement. Continuous monitoring and independent auditing provide assurance, while corrective action and organizational learning feed back into governance and risk assessment.

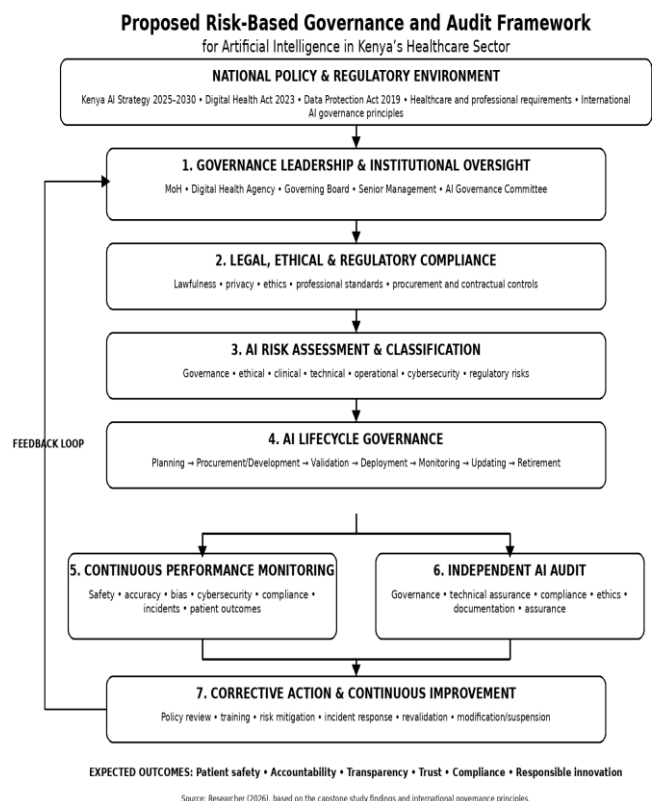


Figure 1. Proposed Risk-Based Governance and Audit Framework for Artificial Intelligence in Kenya's Healthcare Sector

Source: Researcher (2026), based on the capstone findings and international AI governance principles.

4.4 Framework Components

4.4.1 Governance Leadership and Institutional Oversight

The Ministry of Health should provide sector policy leadership and coordination, while the Digital Health Agency should support digital-health implementation and interoperability. Healthcare institutions should establish multidisciplinary AI Governance Committees or equivalent structures. Membership should reflect clinical leadership, ICT, data protection, legal/compliance, risk, quality, ethics, procurement and internal audit expertise, with patient or public-interest representation where appropriate. The committee should maintain an AI register, review risk classifications, approve high-risk deployments, monitor incidents and review audit findings.

4.4.2 Legal, Ethical and Regulatory Compliance

Every AI system should undergo structured compliance review before procurement, development or deployment. Vendor contracts should specify responsibilities for data protection, security, documentation, incident notification, audit evidence, model updates, change control, retention and exit. Compliance should remain continuous; material changes in model, data, intended use, cybersecurity status or law should trigger renewed review.

4.4.3 AI Risk Assessment and Classification

Risk assessment should examine intended purpose, affected populations, decision consequences, data sensitivity, potential harm, governance, ethical, clinical, technical, operational, cybersecurity and regulatory risks. The proposed four-tier classification is: Tier 1 Low/Minimal; Tier 2 Moderate; Tier 3 High; Tier 4 Critical/Unacceptable. The classification is an operational proposal and should undergo expert validation before formal adoption.

4.4.4 AI Lifecycle Governance

Governance should cover planning and needs assessment, procurement or development, data governance, technical and clinical validation, deployment, operation, monitoring, incident management, updating, retraining, change control and retirement. A material change should trigger reassessment of the system's risk profile.

4.4.5 Ethical and Clinical Oversight

High-impact systems should have meaningful human oversight. Responsible professionals must have the competence, authority, information and time needed to question or override AI outputs. Ethical review should examine autonomy, fairness, non-discrimination, explainability, consent where applicable, clinical validity and patient safety. AI should support rather than improperly replace professional judgement.

4.4.6 Continuous Monitoring and Performance Management

Monitoring should cover clinical performance, accuracy where relevant, model or data drift, bias indicators, cybersecurity events, regulatory compliance, incidents, user complaints and patient outcomes. Monitoring frequency should be proportional to risk. A centralized AI register should capture ownership, risk tier, data sources, validation status, version history, monitoring indicators, incidents, audit dates and corrective actions.

4.4.7 Independent Artificial Intelligence Audit

Independent AI auditing should assess at least four dimensions: governance, technical assurance, compliance and ethics. Governance audit examines roles, approvals and controls; technical audit examines data quality, model performance, robustness and cybersecurity; compliance audit examines legal, regulatory, contractual and institutional requirements; ethics audit examines fairness, transparency, explainability, human oversight and patient rights. Audit findings should be graded and linked to corrective-action plans.

4.4.8 Continuous Learning and Framework Improvement

Audit findings, incidents, stakeholder feedback, staff experience, technological developments and regulatory changes should inform periodic review of AI policies, risk classifications, training, monitoring thresholds, audit procedures and vendor arrangements. The aim is to prevent governance from becoming a static compliance document.

4.5 Proposed Risk Classification

Risk tier	Characteristics	Minimum governance response	Illustrative examples
Tier 1 – Low/Minimal	Limited patient impact; mainly administrative/supportive; failure unlikely to cause material harm.	Registration, privacy/security review, training and periodic monitoring.	Low-impact administrative automation.
Tier 2 – Moderate	May influence service delivery or resource	Documented risk	Forecasting, scheduling

Risk tier	Characteristics	Minimum governance response	Illustrative examples
	decisions without directly determining high-impact clinical decisions.	assessment, governance approval, testing, human oversight and periodic internal review.	and limited decision support.
Tier 3 – High	May materially influence diagnosis, treatment, triage, prioritization, monitoring or access to essential care.	Multidisciplinary approval, clinical validation, enhanced bias/data assessment, human oversight, strong cybersecurity, continuous monitoring and independent audit.	Clinical decision-support, diagnostic or predictive systems with material patient impact.
Tier 4 – Critical/Unacceptable	Potential for severe or irreversible harm, unacceptable loss of human control or inability to provide adequate assurance.	Do not deploy until risks are reduced to an acceptable level; prohibit or withdraw use where risk remains unacceptable.	Use cases where safety, accountability or human-rights protections cannot be adequately assured.

4.6 Audit Architecture

The audit architecture is designed to provide independent assurance rather than simply repeat operational monitoring. Governance audit should verify that the institution has approved policies, roles, risk assessments and accountability arrangements. Technical audit should examine data, model performance, robustness, cybersecurity and validation evidence. Compliance audit should test legal, regulatory, contractual and institutional obligations. Ethics audit should examine fairness, transparency, explainability, human oversight, patient rights and evidence of unintended harm.

4.7 Framework Feedback Loop

The framework is deliberately cyclical. Monitoring and audit findings may trigger corrective action, renewed risk assessment, revalidation, modification, suspension or retirement. This feedback mechanism is essential because AI systems operate in changing environments and their risk profile can change as data, models, use cases, technology, regulation or clinical practice changes.

5. IMPLEMENTATION STRATEGIES

5.1 National-Level Implementation

- Develop healthcare-specific AI governance guidelines and implementation standards that complement existing legislation.
- Establish clear coordination mechanisms among the Ministry of Health, Digital Health Agency, data-protection authorities, professional regulators and other relevant institutions.
- Develop a national approach to AI risk classification and assurance for healthcare applications.
- Promote national capacity building in AI governance, AI auditing, cybersecurity, data governance and AI ethics.
- Develop guidance for public-sector procurement of high-risk AI systems, including documentation, audit access, security, update and exit requirements.

5.2 Institutional Implementation

- Establish an AI Governance Committee or equivalent multidisciplinary structure.
- Create and maintain an institutional AI register.
- Integrate AI risk into enterprise risk management, clinical governance, information security and internal audit.
- Require risk assessment before procurement, development or deployment.
- Establish formal validation, monitoring, incident management and audit procedures.
- Ensure staff using AI systems receive appropriate training and understand limitations and escalation procedures.

5.3 Procurement and Vendor Management

AI procurement should include due diligence on data provenance, model performance, security, documentation, explainability, human oversight, incident reporting, audit rights, model updates, change control, data retention and system exit. Contracts should not prevent healthcare institutions or regulators from obtaining the evidence required for safety, compliance and independent assurance.

5.4 Workforce and Capacity Development

Implementation requires more than specialist data scientists. Healthcare organizations need clinicians who understand AI limitations, managers who understand governance, auditors who understand algorithmic assurance, legal and compliance personnel familiar with AI risks and ICT teams capable of managing cybersecurity and data governance. AI literacy should therefore be integrated into professional development and institutional training.

5.5 Phased Implementation Roadmap

Phase	Core activities
Phase 1: Preparation	Policy mapping; institutional readiness assessment; stakeholder engagement; governance structure; AI register.
Phase 2: Governance Establishment	Approve institutional AI policy; establish risk classification; define roles; develop procurement and compliance controls.
Phase 3: Controlled Piloting	Apply the framework to selected AI use cases; conduct validation; establish monitoring and audit processes.
Phase 4: Scale-up	Expand across facilities and counties based on lessons, institutional capacity and risk.
Phase 5: Institutionalization	Embed AI governance into routine regulation, clinical governance, enterprise risk management, internal audit and continuous improvement.

6. POLICY RECOMMENDATIONS

6.1 Government and Policymakers

- Kenya should complement its existing AI and digital-health policy architecture with healthcare-specific AI governance guidance. The guidance should define risk classification, accountability, lifecycle requirements, documentation, human oversight, independent auditing, incident reporting and post-deployment monitoring.

6.2 Ministry of Health

- The Ministry should provide sector leadership for healthcare AI governance, coordinate stakeholders, develop implementation guidance and promote equitable institutional readiness across national and county facilities.

6.3 Digital Health Agency

- The Digital Health Agency should integrate AI governance requirements into digital-health architecture, interoperability, system registration and information-management processes.

6.4 Data Protection and Privacy Oversight

- AI governance should be aligned with data-protection requirements from the earliest stages of system design and procurement. Institutions should ensure that sensitive health data are processed lawfully, securely and only for legitimate purposes.

6.5 Healthcare Institutions

- Healthcare institutions should treat AI governance as an institutional responsibility. Boards, senior management, clinical leadership, ICT, procurement, risk management, ethics, legal/compliance and internal audit should have clearly defined responsibilities.

6.6 AI Developers and Vendors

- Developers should provide sufficient documentation, validation evidence, security controls, information about data and limitations, update procedures and mechanisms for incident reporting and audit. Vendors should be expected to support accountability rather than create information asymmetry that prevents effective assurance.

6.7 Professional Bodies

- Professional regulatory bodies should clarify the responsibilities of healthcare professionals using AI-supported systems and reinforce the principle that professional accountability cannot be displaced simply because a recommendation originated from an AI system.

6.8 Universities and Researchers

- Universities should strengthen interdisciplinary training and research in AI governance, healthcare AI auditing, ethics, cybersecurity, data governance and responsible innovation. Future research should also evaluate the proposed framework empirically in healthcare institutions and county systems.

7. RISKS, LIMITATIONS AND VALIDATION PRIORITIES

7.1 Risks to Implementation

- Limited institutional resources and uneven digital maturity.
- Shortages of AI governance, audit, cybersecurity and data-management skills.
- Fragmented institutional mandates and possible duplication of regulatory responsibilities.
- Rapid technological change that can outpace policy and governance mechanisms.
- Vendor dependence and limited access to proprietary technical information.
- Resistance to change or inappropriate reliance on AI outputs.
- Risk that governance requirements become compliance paperwork rather than active controls.

7.2 Limitations of the Capstone

- The capstone is desk-based and therefore does not provide primary empirical validation from Kenyan healthcare institutions or experts. The local empirical evidence base is also still developing. In addition, AI technologies, international standards and regulatory approaches continue to evolve. The proposed risk classification and governance mechanisms should therefore be treated as a structured policy and implementation proposal requiring further expert validation before formal adoption.

7.3 Validation Priorities

- The framework should be subjected to structured expert review involving healthcare governance, clinical practice, digital health, data protection, cybersecurity, AI development, ethics, legal/compliance, risk management and internal audit. Validation should assess relevance, completeness, clarity, feasibility,

proportionality, institutional accountability, patient safety, legal alignment, auditability and adaptability.

8. CONCLUSIONS

- The capstone demonstrates that Kenya is moving towards increasingly AI-enabled healthcare, but the development of governance capacity has not fully kept pace with technological adoption. The principal challenge is not the absence of all relevant laws and policies; rather, it is the absence of an integrated operational mechanism that translates existing legal, ethical and policy commitments into proportional, auditable and lifecycle-based controls.
- The study concludes that AI risks in healthcare are interconnected. Governance, ethical, technical, operational and regulatory risks can reinforce one another and ultimately affect patient safety, institutional accountability and public trust. Effective governance must therefore combine risk assessment, ethical oversight, legal compliance, technical assurance, human oversight, continuous monitoring and independent auditing.
- The comparative review demonstrates that international frameworks provide valuable but complementary lessons. WHO contributes healthcare-specific ethics; OECD contributes trustworthy AI and risk principles; the EU AI Act contributes risk-based regulatory thinking; NIST contributes operational lifecycle risk management; and ISO/IEC 42001 contributes an organizational management-system approach. Kenya should adapt these strengths to its own legal, institutional and healthcare realities.
- The proposed Risk-Based Governance and Audit Framework provides the principal practical contribution of the capstone. It establishes a coherent governance cycle from readiness assessment and governance establishment through risk classification, compliance, validation, controlled deployment, monitoring, independent audit and continuous improvement. Its value lies in connecting principles to institutional actions and assurance mechanisms.
- Ultimately, the safe and trustworthy adoption of AI in Kenya's healthcare sector will depend on whether governance is treated as an ongoing institutional capability rather than a one-time approval requirement. The proposed framework provides a reference architecture for making that transition while supporting responsible innovation, patient safety, accountability, transparency and public trust.

9. REFERENCES

- African Union. (2024). Continental Artificial Intelligence Strategy. African Union Commission.
- Al Kuwaiti, A., Nazer, K., Al-Reedy, A., Al-Shehri, S., Al-Muhanna, A., Subbarayalu, A. V., Al-Muhanna, A., & Ali, A. (2023). A review of the role of artificial intelligence in healthcare. *Healthcare*, 11(6), 951.
- Aven, T., & Renn, O. (2018). Improving government policy on risk: Eight key principles. *Reliability Engineering & System Safety*, 176, 230–241.
- Bouderhem, R. (2024). Shaping the future of AI in healthcare through ethics and governance. *Humanities and Social Sciences Communications*, 11, Article 416.
- Chaffin, B. C., Gosnell, H., & Cosens, B. A. (2014). A decade of adaptive governance scholarship: Synthesis and future directions. *Ecology and Society*, 19(3), Article 56.
- Davenport, T. H., & Kalakota, R. (2019). The potential for artificial intelligence in healthcare. *Future Healthcare Journal*, 6(2), 94–98.
- Davidson, S., Karlen, W., & Wiens, J. (2024). Governing artificial intelligence in healthcare: Institutional challenges and opportunities. *Frontiers in Artificial Intelligence*, 7, Article 1362108.
- Ebers, M. (2024). The European Union Artificial Intelligence Act: A risk-based regulation for trustworthy artificial intelligence. *Computer Law & Security Review*, 53, 106018.
- Floridi, L., Cowls, J., King, T. C., & Taddeo, M. (2022). How to design AI for social good: Seven essential factors. *Science and Engineering Ethics*, 28(3), 1–19.
- Hashiguchi, T. C. O., Slawomirski, L., & Oderkirk, J. (2021). Laying the foundations for artificial intelligence in health. OECD Health Working Paper No. 128. OECD Publishing.
- Hassan, M., Borycki, E. M., & Kushniruk, A. W. (2025). Artificial intelligence governance framework for healthcare. *Healthcare Management Forum*, 38(2), 90–97.
- Hussein, R., Zink, A., Ramadan, B., Howard, F. M., Hightower, M., Shah, S., et al. (2026). Advancing healthcare AI governance through a comprehensive maturity model based on systematic review. *npj Digital Medicine*, 9, Article 236.
- International Organization for Standardization. (2023). ISO/IEC 42001:2023, Information technology, Artificial intelligence, Management system. ISO.
- Makori, A., Nyongesa, H., & Mugo, P. (2023). Data governance and digital health regulation in Kenya: Implications for artificial intelligence adoption. *BMC Medical Informatics and Decision Making*, 23, Article 312.
- Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics*, 2(3), 603–609.
- Manya, A., Ochieng, J., & Omolo, B. (2024). Digital health transformation and artificial intelligence adoption in Kenya: Opportunities and implementation challenges. *Frontiers in Digital Health*, 6, Article 1362841.
- Mennella, C., Maniscalco, U., De Pietro, G., & Esposito, M. (2024). Ethical and regulatory challenges of AI technologies in healthcare: A narrative review. *Heliyon*, 10(4), e26297.
- Mittelstadt, B. D. (2023). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 5(1), 8–10.
- Mökander, J., Morley, J., Taddeo, M., & Floridi, L. (2023). Ethics-based auditing of automated decision-making systems: Nature, scope and limitations. *AI and Ethics*, 3(2), 405–417.
- Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2024). From principles to practice: Operationalising trustworthy artificial intelligence in healthcare. *npj Digital Medicine*, 7(1).
- Ministry of Information, Communications and the Digital Economy. (2025). Kenya Artificial Intelligence Strategy 2025–2030. Government of Kenya.
- Mugambi, M., Wanyama, P., & Njoroge, E. (2023). Artificial intelligence governance in Kenya's healthcare system: Challenges and future directions. *Frontiers in Artificial Intelligence*, 6.
- Muthee, V., Mugo, D., & Kariuki, S. (2024). Readiness for artificial intelligence implementation in healthcare systems in low- and middle-income

- countries: Evidence from Kenya. *BMC Health Services Research*, 24, Article 412.
- Muthoni, P., Kiplagat, J., & Mwangi, P. (2024). Artificial intelligence and digital innovation in Kenya's healthcare ecosystem. *PLOS Digital Health*, 3(2), e0000418.
- Mwai, P., Ochieng, J., & Wambua, S. (2025). Artificial intelligence governance and digital health transformation in Kenya: Opportunities, challenges and future directions. *African Journal of Health Informatics*, 12(1), 45–61.
- National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce.
- Okech, T. C., Nyaboga, Y., & Kiruja, J. (2023). Digital transformation and artificial intelligence in healthcare delivery in Kenya. *BMC Medical Informatics and Decision Making*, 23, Article 287.
- Organisation for Economic Co-operation and Development. (2024). OECD framework for the classification of AI systems: A tool for effective AI policies.
- Owoyemi, A., Owoyemi, J., Osiyemi, A., & Boyd, A. (2024). Artificial intelligence for healthcare in Africa: Opportunities, challenges and governance considerations. *Frontiers in Digital Health*, 6, Article 1365220.
- Raji, I. D., Smart, A., White, R. N., et al. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. *Proceedings of the 2020 Conference on Fairness, Accountability and Transparency*, 33–44.
- Republic of Kenya. (2019). Data Protection Act, 2019. Government Printer.
- Republic of Kenya. (2023). Digital Health Act, 2023. Government Printer.
- Republic of Kenya. (2025). Kenya National Artificial Intelligence Strategy 2025–2030. Ministry of Information, Communications and the Digital Economy.
- Renn, O. (2021). The IRGC risk governance framework: Revisiting emerging risk governance. *Journal of Risk Research*, 24(9), 1081–1098.
- Shneiderman, B. (2022). Human-centered AI: A framework for reliable, safe and trustworthy systems. *International Journal of Human–Computer Interaction*, 38(6), 495–504.
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339.
- Templin, T., Fort, S., Padmanabham, P., et al. (2025). Framework for bias evaluation in large language models in healthcare settings. *npj Digital Medicine*, 8, Article 414.
- The Lancet Digital Health Commission. (2024). Governing health futures in the age of artificial intelligence. *The Lancet Digital Health*, 6(4).
- Topol, E. (2019). Deep medicine: How artificial intelligence can make healthcare human again. Basic Books.
- Veale, M., & Borgesius, F. Z. (2021). Demystifying the draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112.
- Waiganjo, P., Wambua, S., & Kibet, R. (2024). Digital health policy and artificial intelligence readiness in Kenya. *BMJ Health & Care Informatics*, 31(1), e100921.
- Wang, A., Freeman, S., & Magrabi, F. (2026). Governance for safe and responsible AI in healthcare organisations: A scoping review of frameworks. *npj Digital Medicine*, 9, Article 516.
- World Health Organization. (2021). Ethics and governance of artificial intelligence for health. World Health Organization.