Data Sovereignty Versus Cloud Dependency: Governance Challenges for African Health AI

Brighton Mukundwi
Yeshiva University - Data Analytics and Visualization

ABSTRACT

The digital transformation of African healthcare systems, driven by electronic health records, mobile health platforms, and artificial intelligence, presents substantial opportunities for innovation and efficiency but also poses major governance challenges. The core tension lies between upholding local data sovereignty, the right of countries to govern health data generated within their borders, and dealing with the functional demands of cloud-based AI solutions, which often require cross-border data flows and centralised processing. This paper argues that the fundamental governance challenge for African healthcare infrastructure is balancing sovereignty over health data with the adoption of cloud-based AI. Drawing on a comprehensive literature review of peer-reviewed publications from 2018 to 2026 on data sovereignty, cloud dependencies, AI governance, and African healthcare systems, the paper analyses regulatory frameworks, empirical case studies, and governance models across the continent. The study shows fragmented regulations across 54 African nations, insufficient legal protection for sensitive health data, gaps in ethical consent, infrastructural barriers, and the persistent risk of external control over African health data. Balancing the gains of cloud-enabled AI and the imperatives of privacy, equity, and self-determination is unavoidable. However, hybrid governance models, as demonstrated in Malawi, South Africa, Kenya, and Ethiopia, can reconcile these tensions, enabling innovation without sacrificing sovereignty. The study concludes that African nations must design context-specific governance frameworks that embed data sovereignty within cloud-based health AI from inception. It is recommended that regional data protection laws be harmonised, privacy-preserving AI technologies be adopted, public-private partnerships be established with robust sovereignty safeguards, local data governance capacity be invested in, and participatory models involving local communities be implemented. These strategies are essential for African health systems to realise the benefits of AI-driven transformation while upholding data sovereignty, privacy, and equity.

Keywords

Data Sovereignty, Cloud Computing, Artificial Intelligence, Healthcare Governance, Digital Health, Africa, Data Protection, Health Information Systems, Data Colonialism, Federated Learning

1. INTRODUCTION

The digital transformation of Africa's healthcare systems offers great opportunities to improve health outcomes. Electronic health records (EHRs), mobile health (mHealth) platforms, telemedicine, and artificial intelligence (AI)-powered analytics promise to address longstanding challenges, including access, quality, and efficiency in African healthcare [1, 2]. However, this transformation unfolds within a complex governance landscape characterised by tensions between local data sovereignty and the technical architectures of cloud-based AI systems. Data sovereignty means that data should be subject to the laws, governance structures, and interests of its nation or community of origin, a major issue for African nations seeking to protect citizens' health information as they join the global digital health ecosystem [3]. This challenge is not exclusively technical or legal; it also reflects deeper concerns about digital colonialism, in which outside organisations may extract value from African data without providing proportional benefits to African populations [5, 6]. Africa's history of colonialism and resource extraction increases urgency around who controls, benefits from, and governs the continent's health data [1]. At the same time, modern AI systems promote centralised, cloud-based architectures: machine learning models require large, diverse datasets, and cloud platforms provide scalability, computational power, and cost efficiencies that are difficult to replicate with local infrastructure [7, 8]. According to Apiko and Musoni [9] and López, Rico-Olarte, Blobel, and Hullin [10], Major tech firms and research institutions, mostly based outside Africa, have developed sophisticated AI tools for medical imaging, disease prediction, and decision support. These tools could benefit African healthcare. Their use often requires sending sensitive health data across borders to foreign cloud servers, raising key questions about privacy, security, equity, and sovereignty [3]. This paper examines the governance challenges at the intersection of data sovereignty and cloud dependency in African health AI. The analysis explores the regulatory, technical, ethical, and socio-political dimensions, drawing on evidence from multiple African contexts, demonstrating that the sovereignty-cloud debate is not a simple binary choice but a landscape of trade-offs, hybrid solutions, and context-specific governance.

Africa's 54 nations show varied economic development, regulatory structures, health infrastructure, and digital readiness, making no single governance model suitable for all [11, 12]. However, common challenges and promising practices can still guide policy. For example, Malawi, South Africa, Kenya, and Ethiopia illustrate different balances of sovereignty and cloud-based innovation, offering useful lessons [13, 14, 15]. This paper advances a central argument: that data sovereignty should be central to the governance of cloud-dependent health AI in African nations. First, the analysis addresses governance challenges as African nations navigate data sovereignty and cloud dependency, considering regulatory, technical, ethical, and infrastructural dimensions. Second, case studies illustrate successes and ongoing challenges across different governance approaches. Third, a multi-level governance framework is proposed that embeds sovereignty principles into cloud-based health AI systems from the outset, offering recommendations for policymakers, healthcare institutions, technology providers, and civil society organisations.

COVID-19 accelerated the digitalisation of health care across Africa, prompting many countries to rapidly adopt cloud-based surveillance, contact tracing, and vaccine management [16, 17]. However, this rapid growth largely occurred without

robust governance, leading to practices that may be difficult to reverse. The data governance decisions made now will shape African health systems for years to come.

The structure of this analysis is as follows. Section 2 provides background on data sovereignty, cloud computing, AI in healthcare, and the African healthcare landscape. Section 3 examines core governance challenges related to sovereignty and cloud dependency. Section 4 reviews the trade-offs and tensions in various governance approaches. Section 5 presents detailed African case studies. Section 6 covers emerging solutions and best practices, followed by Section 7's comprehensive governance framework. Section 8 discusses implications and limitations, and Section 9 concludes with policy and practice recommendations.

2 BACKGROUND AND THEORETICAL FOUNDATIONS

2.1 Data Sovereignty in the Digital Age

'Data sovereignty' has grown from a narrow legal concept, namely, jurisdiction over data, to a wider notion involving control, ownership, and authority over how data is collected, stored, processed, and shared [2, 18]. In the context of health data, data sovereignty specifically addresses the rights to privacy, autonomy, and informed consent regarding the use of data. In Africa, it further encompasses goals of economic development, technological self-reliance, and resistance to digital resource extraction reminiscent of colonial practices [5, 19].

The principle of data sovereignty rests on several arguments. First, health data is highly sensitive and contains personally identifiable information, health behaviours, and vulnerabilities. Governments have a core responsibility to safeguard this data against unapproved access, misuse, or exploitation [20]. Second, health data has major economic value; the global health data market is projected to reach hundreds of billions of dollars. African nations seek to ensure that the value derived from their populations' data returns to those populations [21]. Third, data sovereignty underpins public trust in digital health systems. Without assured data protections, citizens may be hesitant to adopt new technologies [7, 14]. However, data sovereignty is not absolute. Strict localisation requirements, such as policies mandating that all data remain within national borders, could restrict research and access to advanced AI tools and raise costs for resource-limited health systems [8]. The challenge is to define sovereignty in a way that protects legitimate interests while also enabling beneficial data flows and innovation.

2.2 Cloud Computing and AI in Healthcare

Cloud computing has become the dominant paradigm for modern digital infrastructure. It offers on-demand access to computational resources, storage, and software services. Organisations do not have to build and maintain their own data centres [22]. For healthcare systems in resource-constrained settings, cloud computing offers advantages. These include reduced capital expenditure, scalability, automatic software updates, and access to advanced analytics [14, 23]. Artificial intelligence in healthcare relies heavily on cloud infrastructure. First, training advanced machine learning models needs substantial computational power. This commonly includes graphics processing units (GPUs) or AI accelerators, which are costly to maintain locally [24]. Second, AI models require large, diverse training datasets. Cloud platforms facilitate the aggregation of data across multiple sites [5, 25]. Third, deploying AI models at scale requires robust infrastructure for model serving, monitoring, and updating. Cloud platforms provide this efficiently [25].

However, cloud-based AI in healthcare introduces significant cybersecurity, sovereignty, and operational risks. Data in cloud environments may be exposed to data breaches, unauthorised access, or surveillance by cloud providers or government authorities [2]. Cloud services are dominated by a few multinational technology companies headquartered outside Africa, leading to foreign dependency and creating potential single points of failure [1]. Service interruptions stemming from technical outages, cyberattacks, or geopolitical instability may disrupt the fundamental delivery of healthcare [7]. For African health systems, these external dependencies are especially critical. Most major cloud providers maintain minimal infrastructure on the continent, requiring data transmission to and storage in overseas data centres [8]. This results in higher latency, greater vulnerability to interregional network failures, and subjection of data to extraterritorial legal regimes. The concentration of AI technical expertise and resources in select international hubs intensifies these problems. AI models may lack adequate representation of African population diversity, disease profiles, or health system contexts [6, 9].

2.3 The African Healthcare Context

To understand governance challenges in African health AI, it is important to appreciate the continent's diverse healthcare landscape. Africa has 54 nations, with populations ranging from under one million to over 200 million [14]. Gross domestic product (GDP) per capita ranges from under $500 to over $20,000, and healthcare systems are at different stages of development [11]. Some countries have near-universal health coverage with sophisticated digital health infrastructure. Others struggle with basic service delivery and minimal digital capability [12].

Several common challenges characterise many African healthcare systems. First, resource constraints limit investments in health infrastructure, workforce, and technology [10]. Second, fragmented health information systems, often consisting of multiple vertical programs with incompatible data systems, impede comprehensive patient care and population health management [11]. Third, infrastructure deficits in electricity, internet connectivity, and technical capacity constrain the implementation of digital health [7, 8]. Fourth, weak regulatory frameworks and limited enforcement capacity create governance gaps [18]. Despite these challenges, Africa has demonstrated remarkable innovation in digital health. The continent has been a global leader in mobile health, with pioneering initiatives in mobile money, SMS-based health information, and digital tools for community health workers [12]. Several African countries have implemented national health information exchanges and are advancing toward universal health coverage through digital means. The COVID-19 pandemic catalysed the rapid adoption of digital surveillance, telemedicine, and vaccine management systems [16, 17].

The diversity of African contexts necessitates governance solutions that are adaptable and context-specific. A governance framework appropriate for South Africa, with relatively advanced infrastructure, regulatory capacity, and technical expertise, may not be feasible for countries with more limited resources [14]. Regional economic communities, such as the African Union, Economic Community of West African States (ECOWAS), and Southern African Development Community (SADC), play important roles in harmonising approaches and facilitating cross-border collaboration [23].

3 METHODOLOGY

This study is based on a structured qualitative literature review designed to map the governance challenges emerging at the intersection of data sovereignty, cloud computing, and artificial intelligence in African healthcare systems. Rather than conducting an exhaustive systematic review, the approach followed a targeted, thematic synthesis strategy, as recommended by [26], which prioritises conceptual clarity and policy relevance in emerging interdisciplinary fields. The review sought to identify peer-reviewed scholarship, legal analyses, and policy documents addressing digital health governance, AI regulation, data localisation, and digital colonialism. The objective was not merely descriptive aggregation but analytical integration, allowing the identification of patterns of institutional tension and governance responses across legal, technical, and political-economy domains.

The literature search was conducted across four primary databases: African Journals Online, Scopus, Web of Science, and PubMed. Search strings combined keywords such as "data sovereignty," "health data governance," "AI in healthcare Africa," "cloud computing regulation," "digital colonialism," and "data localisation." Boolean operators were applied to refine search outputs. Initial screening was conducted based on titles and abstracts, followed by full-text review where relevance to African governance contexts was evident.

The time frame of 2018-2026 was deliberately selected to capture the period following the acceleration of AI deployment in healthcare and the increasing prominence of data sovereignty debates in African regulatory discourse. As van Reisen et al [17] notes, the COVID-19 pandemic significantly intensified digital health adoption, making post-2018 scholarship particularly salient. Earlier foundational works were consulted selectively where necessary for theoretical grounding, but the core dataset focused on contemporary developments reflecting current technological capacity and regulatory evolution. This bounded time frame enhances analytical relevance while ensuring that conclusions reflect the present governance landscape rather than outdated infrastructure assumptions.

Inclusion criteria required that publications directly address at least one of the following: (1) AI governance in healthcare, (2) data localisation or sovereignty law, (3) cloud infrastructure regulation, or (4) African digital health systems. Exclusion criteria: purely technical AI studies without governance implications, and non-African case studies, unless used for comparative insight. Thematic coding was conducted iteratively, identifying recurring tensions between efficiency, performance, sovereignty, and collaboration. These themes subsequently informed the development of the Framework presented in Section 7.

4 GOVERNANCE CHALLENGES AT THE INTERSECTION OF SOVEREIGNTY AND CLOUD DEPENDENCY

4.1 Fragmented Regulatory Landscapes

One of the most significant governance challenges facing African health AI is the fragmented and often inadequate regulatory landscape for data protection and digital health. While some African nations have enacted comprehensive data protection laws, such as South Africa's Protection of Personal Information Act (POPIA) and Kenya's Data Protection Act, many countries lack specific legislation governing health data [4, 27]. Even where laws exist, enforcement capacity is often limited, and regulations may not adequately address the specific challenges posed by AI and cloud computing [18]. The fragmentation operates at multiple levels. At the national level, responsibility for health data governance is often distributed across multiple agencies, ministries of health, information and communications technology regulators, data protection authorities, and others, without clear coordination mechanisms [2]. This creates confusion about which entity has authority over different aspects of health AI governance, potentially resulting in regulatory gaps or conflicts.

At the continental level, the lack of harmonisation across African nations creates challenges for regional health initiatives and cross-border data flows. The African Union has developed frameworks such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), but ratification and implementation have been slow [23]. Countries have adopted varying approaches to data localisation, cross-border data transfer restrictions, and consent requirements, creating a patchwork that is difficult for healthcare organisations and technology providers to navigate [2].

The regulatory fragmentation is particularly problematic for AI systems, which often require data from multiple countries to achieve adequate diversity and performance. A diagnostic AI model trained only on data from a single country may not generalise well to populations in other countries with different disease prevalence, genetic backgrounds, or healthcare practices [9]. However, aggregating data across borders requires navigating multiple regulatory regimes, each with different requirements for consent, data protection, and cross-border transfer [4].

Several African countries have begun to address these challenges through regulatory development and regional harmonisation efforts. South Africa's AI policy framework explicitly addresses data sovereignty and cross-border data flows, proposing mechanisms for international data sharing with appropriate safeguards [27]. The East African Community has developed a framework for harmonising data protection laws across member states [23]. However, implementation remains uneven, and significant gaps persist.

4.2 Infrastructural and Technical Constraints

Infrastructure deficits represent a fundamental constraint on African nations' ability to implement data sovereignty principles while leveraging cloud-based AI. Data sovereignty ideally requires local infrastructure capable of storing, processing, and analysing health data within national borders. However, many African countries lack reliable electricity, internet connectivity, data centre capacity, and the technical expertise necessary for such infrastructure [7].

Electricity access and reliability remain significant challenges across much of Africa. While urban areas in many countries have relatively reliable power, rural areas, where much of the population lives, often experience frequent outages or lack grid access entirely [7]. Healthcare facilities in rural areas may rely on generators or solar power, which may not provide sufficient or consistent power for data-intensive computing [8]. Cloud-based solutions, which shift computational demands to remote data centres, can mitigate some of these local infrastructure constraints, but they require reliable internet connectivity.

Internet connectivity in Africa has improved dramatically over the past decade, with submarine fibre optic cables connecting the continent to global networks and mobile broadband expanding rapidly [12]. However, connectivity remains expensive, unreliable, and unevenly distributed. Many healthcare facilities, particularly in rural areas, lack high-speed

internet access [8]. Even when connectivity is available, bandwidth may be insufficient to transmit large medical imaging files or support real-time AI inference [7]. Latency, the delay in data transmission, can be problematic for time-sensitive clinical applications when data must travel to distant cloud servers and back [15].

Data centre infrastructure within Africa is limited compared to other regions. While South Africa, Kenya, Nigeria, and a few other countries have developed commercial data centre capacity, much of the continent lacks local facilities [8]. This means that cloud services often rely on data centres located in Europe, North America, or Asia, subjecting data to foreign jurisdictions and creating dependencies on international network connections [2]. Building local data centre capacity requires substantial investment in facilities, cooling systems, power infrastructure, and security, investments that may be difficult to justify given limited resources and competing priorities [7].

Technical capacity, the availability of skilled personnel to design, implement, and maintain health AI systems, is another critical constraint. African countries face significant shortages of data scientists, AI engineers, cybersecurity specialists, and health informatics professionals [24]. This skills gap makes it difficult to develop local AI capabilities and to effectively govern and oversee cloud-based systems provided by external vendors. Brain drain, with skilled professionals emigrating to higher-income countries, exacerbates this challenge [24].

These infrastructural and technical constraints create a dependency dilemma. Local infrastructure is insufficient to fully implement data sovereignty principles, prompting countries to adopt cloud-based solutions. However, reliance on cloud services, particularly those provided by foreign companies, undermines sovereignty and creates new dependencies. Breaking this cycle requires strategic investments in infrastructure and capacity building, but such investments compete with immediate healthcare needs in resource-constrained environments [10].

4.3 Data Colonialism and Power Asymmetries

The concept of "data colonialism" has emerged as a critical lens for understanding power dynamics in global digital health [5]. Data colonialism refers to the appropriation of data from populations in low- and middle-income countries by actors in high-income countries, often with minimal benefit flowing back to the data subjects or their communities. This pattern mirrors historical colonial extraction of natural resources, but with data as the extracted commodity [5].

In the context of African health AI, data colonialism manifests in several ways. First, research partnerships between African institutions and well-resourced institutions in high-income countries often involve the transfer of African data to foreign institutions for analysis, with African partners having limited control over how the data are used or who benefits from the resulting intellectual property [5, 24]. Second, technology companies offering "free" or low-cost digital health tools may extract value from the data generated by those tools, using African health data to train AI models that are then commercialised globally without sharing profits with data sources [5]. Third, global health initiatives and humanitarian organisations may collect extensive health data during emergencies or interventions without establishing clear governance structures for long-term data stewardship [17].

Power asymmetries between African institutions and global technology companies create challenges for negotiating equitable data governance arrangements. Large technology companies have sophisticated legal teams, extensive resources, and market power that African governments and healthcare institutions often cannot match [1]. Standard terms of service for cloud platforms may include provisions that grant providers broad rights to access, analyse, or share data in ways that conflict with sovereignty principles [2]. African institutions may lack the technical expertise to fully understand the implications of complex data processing agreements or to effectively audit compliance [24]. The concentration of AI development capacity in a few global centres creates additional asymmetries. Most advanced AI models for healthcare are developed by institutions in the United States, Europe, or China, using datasets that predominantly represent populations in those regions [9]. When these models are deployed in African contexts, they may perform poorly due to differences in disease prevalence, genetic backgrounds, healthcare practices, or data quality [9, 25]. However, African institutions often lack the capacity to develop alternative models tailored to local contexts, leading to dependence on potentially inappropriate technologies.

Addressing data colonialism requires more than technical solutions; it demands fundamental shifts in power relations and governance structures. This includes ensuring that African institutions and communities have a meaningful voice in decisions about data governance, that benefits from data use flow back to data sources, and that capacity building enables African actors to develop their own AI capabilities rather than remaining perpetually dependent on external providers.

4.4 Ethical and Cultural Considerations

Ethical governance of health AI in Africa must grapple with complex questions about consent, privacy, equity, and cultural appropriateness. Western bioethical frameworks, which emphasise individual autonomy and informed consent, may not fully align with African cultural contexts that prioritise communal decision-making and collective welfare [20, 27]. This creates tensions in designing consent processes for health data use and AI deployment.

Informed consent for the use of health data in AI systems is particularly challenging. The complexity of AI systems, involving data aggregation, algorithmic processing, and potential secondary uses that may not be fully specified at the time of initial collection, makes it difficult to provide truly informed consent [20]. In contexts with limited health literacy or digital literacy, explaining how AI systems work and what risks they pose is even more challenging [10]. Dynamic consent models, which allow individuals to update their preferences over time as technologies and uses evolve, have been proposed but are difficult to implement at scale [2]. Privacy norms vary across African cultures and contexts. While privacy is valued, it may be conceptualised differently than in Western contexts, with greater emphasis on privacy from outsiders while accepting less privacy within family or community groups [20]. Cloud-based systems designed according to Western privacy models may not align with these cultural norms. Additionally, in contexts where healthcare access is limited, individuals may be willing to trade privacy for access to services, thereby creating a risk of exploitation [5].

Equity considerations are central to the ethical governance of African health AI. AI systems have the potential to reduce health disparities by improving access to diagnostic and treatment capabilities in underserved areas [25]. However, they also risk exacerbating inequities if deployed primarily in urban areas or in private facilities accessible only to wealthier populations, if they perform poorly for marginalised groups, or if they divert resources from other health priorities [10, 25]. Governance frameworks must explicitly address equity

implications and include mechanisms to ensure that AI benefits reach those most in need. Cultural appropriateness extends to the design of AI systems themselves. User interfaces, language options, and interaction modalities must be adapted to local contexts [10]. AI models must be trained on data representative of the populations they will serve, accounting for genetic diversity, disease patterns, and healthcare practices specific to African contexts [5]. Governance processes should include meaningful participation by affected communities, not just technical experts and policymakers [5].

The ethical principle of beneficence, which requires AI systems to do more good than harm, calls for cautious assessment in resource-constrained settings. Investments in AI must be weighed against other health priorities, and the opportunity costs of cloud-based AI dependencies must be considered [10]. Ethical governance requires transparency about trade-offs and inclusive processes for making difficult allocation decisions.

5 TRADE-OFFS AND TENSIONS: SOVEREIGNTY VS. INNOVATION

5.1 Efficiency and Scalability versus Local Control

The conflict between cloud efficiency and sovereign control need not be treated as a zero-sum game, but rather as a problem of governance design that must be addressed at multiple levels. Although Masana and Muriithi [14] demonstrates that cloud-based electronic medical record systems have a profound impact on scalability and lower capital spending, [2] warns that these efficiencies may weaken jurisdictional power in the face of weak regulatory oversight. Instead of resolving this tension in terms of absolute localisation, policy tools such as the Malabo Convention of the African Union, as discussed by Rayan [23], provide a harmonised model of conditional cross-border transfer based on standards of adequacy and oversight. Federated learning architectures outlined in Tiffin, George, and LeFevre [4] technically offer a complementary approach to distributed model training that does not involve centralising raw data. In cases where hybrid cloud deployment is coupled with the encryption key's custody in the hands of the national body, as suggested by Denboba et al. [7], performance efficiency can align with enforceable sovereignty. In this way, the conflict between efficiency and control is resolved through balanced integration rather than exclusion. Ultimately, this tension is not a deadlock; it can be resolved through the application of 'Accountability and Redress' principles and the deployment of 'Auditing Technologies' detailed in Section 7.

5.2 Performance of the AI model vs the localisation of data

The connection between the performance of models and the localisation of data can also be described as those that require institutional calibration rather than ideological positioning. Apiko and Musoni [9] state that the successful deployment of diagnostic AI systems is data-intensive and requires extensive, heterogeneous datasets, whereas Adewole et al. [11] demonstrates that the use of externally aggregated data can reduce contextual relevance for African populations. This poses a two-fold threat: performance impairment from rigid localisation and contextual bias from free aggregation. A policy option for controlled intra-African data sharing can be pursued through regional regulatory harmonisation, which is premised on the Malabo Convention framework [28]. At the same time, technical tools like transfer learning and federated learning, considered by Tiffin, George, and LeFevre [4], enable the use of globally trained models to be fine-tuned on local datasets without mass data export. Yeng et al. [22] also explain the benefits of synthetic data generation in complementing restricted datasets without violating privacy. By means of coordinated regulatory contracts and privacy-conserving computation, the tension of performance-localisation can be handled as a trade-off, but not as a structural barrier. Technical remedies such as 'Federated Learning' and 'Privacy-Preserving Technologies' (see Section 7.1) allow for high performance without violating the imperatives of national data residency.

5.3 International Cooperation vs. National Interests

International cooperation offers both opportunities for development and risks to sovereignty, but the struggle can be seen only as an asymmetry of governance, not a partnership. Davis [5] emphasised global digital health projects for reproducing extractive data politics, Oladosu et al. [1] highlight the structural imbalance in rewards for cloud service deals. Nevertheless, Tanveer et al. [12] shows that domestic capacities can be enhanced through the use of public-privacy digital ecosystems in the context of contract-based provisions on local ownership and capacity-building. Intellectual property co-ownership, a data residency (assurance), and dispute resolution court enforceable in domestic courts, as proposed by Naidoo et al. [27], turn collaboration into an enforced partnership. At the regional level, Rayan [23] highlights that harmonised governance arrangements make systems less vulnerable by enhancing collective bargaining power. The institutional sequencing to this end then resolves the collaboration-sovereignty tension: uncoordinated reliance poses a threat, while coordinated association under enforceable governance generates a win-win result. Transitioning from extractive dependency to equitable partnership requires the 'Multi-Level Governance Architecture' proposed in Section 8.2, which ensures that collaborative gains do not come at the cost of strategic autonomy.

6 CASE STUDIES: AFRICAN EXPERIENCES WITH HEALTH DATA GOVERNANCE

6.1 Malawi's National Digital Health Information System

Malawi's National Digital Health Information System (NDHIS) represents an innovative approach to balancing data sovereignty with cloud-based infrastructure. Designated as a priority by the Ministry of Health in 2022, the NDHIS employs a cloud-native architecture built on Kubernetes while incorporating trusted computing technologies to maintain data sovereignty [15]. The system uses zero-trust secure communication to protect data confidentiality and integrity during transmission, and trusted computing ensures that data is processed only by certified software, preserving privacy and sovereignty even when using cloud infrastructure. The NDHIS architecture addresses several key governance challenges. By deploying trusted medical information guards as gatekeepers at every computing node, the system maintains local control over data access and processing while leveraging cloud scalability [15]. This approach enables Malawi to offer data rental services to healthcare researchers and AI developers worldwide, generating revenue from data while maintaining sovereignty and without compromising patient privacy or national control. The Malawi case demonstrates that cloud-native architectures and data sovereignty are not inherently incompatible. Through careful design incorporating privacy-preserving technologies and governance-by-design principles, it is possible to achieve both the efficiency of cloud computing and the control required

for sovereignty [15]. However, implementing such sophisticated systems requires technical expertise and international partnerships; Malawi collaborated with Luke International in Norway and technology providers in Taiwan to develop the NDHIS [15].

Challenges remain in scaling the system nationally and ensuring long-term sustainability. The prototype has been tested in connecting community clinics with district hospitals, but expanding to cover Malawi's entire healthcare system will require substantial investment in infrastructure, training, and change management [15]. The system's reliance on international technology partners also creates dependencies that demand cautious management to ensure Malawi retains control and capacity.

6.2 South Africa's AI Policy Development

South Africa has taken a proactive approach to AI governance, developing comprehensive policy frameworks that explicitly address data sovereignty, ethics, and equity [27]. The country's Protection of Personal Information Act (POPIA) provides a strong legal foundation for data protection, and South Africa has been developing AI-specific policies that build on this foundation while addressing the unique challenges of AI in healthcare [27]. South Africa's AI policy framework emphasises several key principles: transparency and explainability of AI systems, fairness and non-discrimination, accountability for AI decisions, and data sovereignty with provisions for international data sharing under appropriate safeguards [27]. The framework recognises that strict data localisation would impede beneficial research and innovation, but establishes clear requirements for cross-border data transfers, including adequacy assessments of recipient countries' data protection regimes and contractual safeguards [27]. In healthcare specifically, South Africa has been developing guidelines for AI deployment that address clinical validation, safety monitoring, and integration with existing health information systems [27]. The country has also invested in building local AI capacity through university programs, research centres, and public-private partnerships [27]. This capacity-building is seen as essential to ensuring that South Africa can effectively govern AI systems rather than remain dependent on external expertise.

However, implementation challenges persist. Enforcement of data protection regulations has been uneven, and many healthcare institutions lack the resources and expertise to fully comply with requirements [27]. The private-public divide in South African healthcare creates additional complexity, with private facilities often having more advanced digital infrastructure but less oversight than public facilities [14]. Ensuring that AI benefits reach underserved populations, particularly in rural areas and townships, remains a significant equity challenge [27].

6.3 Kenya's Cloud-Based Health Service Delivery

Kenya has been a pioneer in digital health innovation, building on its success with mobile money (M-Pesa) to develop sophisticated mobile health platforms [12]. The country has also embraced cloud computing for health service delivery, with several initiatives leveraging cloud infrastructure to improve access and efficiency [8].

A study of public health facilities in Kisumu County, Western Kenya, examined the impacts of cloud computing adoption on health service delivery [8]. The research found that cloud-based systems improved data accessibility, enabled real-time reporting, and facilitated coordination across facilities [8]. However, the study also identified significant challenges, including unreliable internet connectivity, limited technical capacity among health workers, and concerns about data security and privacy [8]. Kenya's experience highlights the importance of infrastructure readiness for cloud-based health systems. While urban areas generally have adequate connectivity, rural facilities often struggle with unreliable or expensive internet access [8]. Power outages and equipment failures can disrupt cloud-based services, presenting risks to the continuity of care [8]. These infrastructural challenges must be addressed for cloud-based AI to be viable across Kenya's diverse healthcare landscape. Kenya has also grappled with data governance challenges in its digital health initiatives. The country enacted a Data Protection Act in 2019, establishing a framework for the protection of personal data and creating a Data Protection Commissioner [4]. However, implementation has been gradual, and many digital health initiatives launched before the Act's passage operate in a regulatory grey area [22]. Ensuring that cloud-based health systems comply with data protection requirements while maintaining efficiency and accessibility remains an ongoing challenge.

Kenya's approach to health data governance emphasises public-private partnerships, with the government working alongside technology companies, NGOs, and development partners to build digital health infrastructure [12]. While these partnerships have accelerated progress, they also create governance complexity and potential conflicts of interest that must be carefully managed [12].

6.4 Ethiopia's Hospital Information Systems

Ethiopia has been working to modernise its healthcare information systems, with particular focus on implementing cloud-based solutions in hospitals. A comprehensive study of Ethiopian hospitals explored challenges and prospects of cloud-based models for healthcare information services [7]. The research identified several key barriers to cloud adoption, including limited internet connectivity, unreliable electricity supply, insufficient technical capacity, and concerns about data security and sovereignty [7]. Despite these challenges, the study found that healthcare professionals and administrators recognised the potential benefits of cloud computing and were generally supportive of its adoption, provided appropriate safeguards [7]. The research proposed a Software-as-a-Service (SaaS) community cloud model tailored to Ethiopian contexts, emphasising local data centres, government oversight, and capacity building [7]. Ethiopia's experience illustrates the infrastructural constraints that many African countries face in implementing cloud-based health AI. While cloud computing offers theoretical advantages, realising them requires baseline infrastructure that may not be available [7]. Investments in electricity, connectivity, and technical training are prerequisites for effective cloud adoption [7]. Ethiopia has also been developing its regulatory framework for digital health and data protection. The country is working on data protection legislation and has established a Digital Transformation Commission to coordinate digital initiatives across sectors [7]. However, regulatory development has lagged behind technological adoption, creating governance gaps [7].

The Ethiopian case underscores the importance of context-appropriate solutions. Rather than simply adopting cloud models designed for high-income countries, Ethiopia is exploring hybrid approaches that combine local infrastructure with selective use of cloud services, prioritising sovereignty and sustainability [7].

6.5 Regional Initiatives and Pan-African Frameworks

Beyond national efforts, regional and continental initiatives are working to harmonise data governance approaches and facilitate cross-border collaboration. The African Union has developed several relevant frameworks, including the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and the Digital Transformation Strategy for Africa [12, 23].

The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), adopted on 27 June 2014, entered into force on 8 June 2023 following the fifteenth instrument of ratification [28]. As of July 2024, sixteen Member States had ratified the Convention, exceeding the threshold required under Article 36. Regional economic communities have also developed data governance frameworks. The East African Community has worked on harmonising data protection laws across member states, and the Economic Community of West African States (ECOWAS) has developed a supplementary act on personal data protection [23]. These regional frameworks aim to facilitate cross-border data flows within regions while maintaining protection standards. The COVID-19 pandemic catalysed several pan-African digital health initiatives. The Africa Centres for Disease Control and Prevention (Africa CDC) developed platforms for surveillance data sharing, and several regional initiatives emerged for vaccine distribution tracking [16]. These initiatives demonstrated both the potential for continental collaboration and the challenges of coordinating across diverse regulatory and technical environments [17].

The Smart Africa Alliance, a partnership of African governments and private sector actors, has been promoting digital transformation across the continent, including in healthcare [12]. The Alliance has developed frameworks for digital health interoperability and data governance, though implementation varies across member countries [12].

6.6 COMPARATIVE ANALYSIS

Country	Infrastructure Level	Primary Governance Focus	Preferred Deployment Model
Malawi	Low / Transitioning	Scalability & Pragmatism	Cloud-native with Trusted Computing
Ethiopia	Basic / State-led	Sovereignty & Control	State-centric / Community SaaS
South Africa	Advanced	Equity, Ethics & Regulation	Hybrid (Public-Private Ecosystem)
Kenya	Moderate / Pioneer	Innovation & Access	Public-Private Alliances / Cloud-based

Although the above case studies exemplify the varied national strategies, a comparative prism shows that governance decisions are influenced less by abstract ideology than by the conditions of the political economy and institutional capacity. The cloud-native strategy used by Malawi reflects what Tanveer et al. [12] term infrastructure-constrained pragmatism, in which there is inadequate domestic data centre capacity and the increasing integration with external providers is a fiscally rational choice. In comparison, Ethiopia's more conservative stance aligns with [7] definition of the state-centric model of digital governance, which emphasises national control and the gradual development of infrastructure, even at the cost of scalability. South Africa can take advantage of somewhat developed regulatory institutions and showcases a hybrid governance model similar to that of mixed public-private digital ecosystems, as analysed by [14]. The history of Kenya, as Tiffin, George, and LeFevre [4] explains, is one of negotiated sovereignty, which capitalises on multinational cloud alliances and, in the process, progressively integrates mechanisms of control. Compounding these cases suggests that fiscal space, regulatory maturity, donor integration, and state centralisation traditions mediate sovereignty strategies. The fact that divergence is inherent to countries further strengthens the main point of this paper: good governance should be based on balancing at a calculated, context-specific level rather than blanket localisation requirements.

7 EMERGING SOLUTIONS AND BEST PRACTICES

7.1 Privacy-Preserving Technologies

Privacy-preserving technologies show potential approaches to enabling AI development while maintaining data sovereignty and protecting individual privacy. Federated learning, differential privacy, homomorphic encryption, and secure multi-party computation are among the techniques being explored for African health AI applications [22].

Federated learning enables AI models to be trained across multiple sites without centralising data. Instead of sending data to a central server, the model is deployed to each site, trained locally, and only model updates (not raw data) are shared with a central coordinator [22]. This approach has been demonstrated in cross-border telemedicine applications in Kenya, where federated learning combined with differential privacy enabled collaborative model development while preserving data sovereignty [22]. Differential privacy adds carefully calibrated noise to data or model outputs to prevent the identification of individual records while preserving statistical properties useful for AI training [22]. This technique can enable data sharing for research and AI development with reduced privacy risks [22]. However, the privacy-utility trade-off inherent in differential privacy means that stronger privacy guarantees reduce data utility and require careful calibration for healthcare applications where accuracy is critical [22].

Moreover, homomorphic encryption enables computations on encrypted data without decryption, supporting cloud-based AI inference while keeping data encrypted throughout processing [22]. This technology is computationally intensive and still evolving, but it offers the potential to uphold data confidentiality even when using untrusted cloud infrastructure [22]. Additionally, Secure multi-party computation enables multiple parties to jointly compute functions over their combined data without revealing their individual inputs to each other [22]. This could enable African countries to collaboratively develop AI models using pooled data while each country maintains sovereignty over its own data [22].

While these technologies are promising, they also present challenges. They require technical expertise that may be

limited in African contexts, can reduce model performance compared to traditional approaches, and may introduce computational overhead that is problematic in low-resource settings [22]. Capacity building and technology transfer are essential for African institutions to effectively deploy privacy-preserving technologies [24].

7.2 Hybrid Cloud Architectures

Hybrid cloud architectures, which combine local infrastructure with selective use of external cloud services, offer a pragmatic approach to balancing sovereignty and cloud benefits [15]. In hybrid models, sensitive data and critical applications are hosted on local infrastructure under direct institutional control, while less sensitive workloads or computationally intensive tasks are offloaded to external cloud services [7].

Several African countries are implementing hybrid approaches. South Africa has developed national health data centres that host core health information systems locally while using international cloud services for specific applications such as AI model training or disaster recovery [14]. This approach maintains sovereignty over primary data while leveraging cloud capabilities where appropriate [14]. Hybrid architectures require careful governance to determine which data and applications should remain local versus which can appropriately use external cloud services. Risk assessment frameworks can guide these decisions, considering factors such as data sensitivity, regulatory requirements, performance needs, and cost [2]. Clear policies and technical controls are needed to prevent unauthorised data migration from local to cloud environments [2].

Edge computing, processing data close to where it is generated rather than in centralised cloud data centres, is another architectural approach relevant to African contexts [21]. Edge computing can reduce latency, decrease bandwidth requirements, and enable continued operation during network disruptions [21]. For AI applications, edge deployment of trained models can enable local inference while training occurs in the cloud [9].

Hybrid architectures also facilitate gradual transitions. Countries can begin with primarily local infrastructure and incrementally adopt cloud services as regulatory frameworks mature, technical capacity develops, and trust is established [7]. This evolutionary approach may be more feasible than implementing comprehensive cloud-based systems immediately [14].

7.3 Participatory Governance Models

Participatory governance models that include affected communities in decision-making about health data and AI represent an important best practice for ensuring that governance frameworks reflect diverse values and interests [5]. Traditional top-down governance approaches, where policies are developed by technical experts and government officials without community input, risk overlooking important ethical and cultural considerations and may lack public legitimacy [5]. Participatory action research approaches have been used in global digital health to engage communities in identifying governance priorities and developing solutions [5]. These approaches recognise that communities affected by digital health systems have valuable knowledge and legitimate interests that should inform governance. Participation can take various forms, from consultation and feedback on proposed policies to co-design of systems and shared decision-making authority [5]. In African contexts, participatory governance must navigate complex questions about representation and inclusion. Who speaks for "the community"? How can marginalised groups, women, rural populations, people with disabilities, and linguistic minorities be meaningfully included? How can participation be structured to be genuinely empowering rather than tokenistic? These questions require careful attention to power dynamics and deliberate efforts to create inclusive processes. Digital platforms can facilitate participation by enabling broader engagement than traditional in-person consultations, but they also risk excluding those without digital access [5]. Hybrid approaches that combine digital and in-person engagement, use multiple languages, and provide support for participation may be necessary to achieve genuine inclusivity [5].

Participatory governance is particularly important for AI systems, which can have significant impacts on individuals and communities but are often opaque and difficult for non-experts to understand [20]. Explaining AI systems in accessible ways, creating opportunities for communities to express concerns and preferences, and establishing accountability mechanisms responsive to community input are essential components of participatory AI governance.

7.4 Capacity Building and Knowledge Transfer

Building local capacity for health AI governance is essential for African countries to move beyond dependency on external expertise and to effectively exercise data sovereignty [24]. Capacity building must occur at multiple levels: individual skills development, institutional capability strengthening, and ecosystem development [24]. At the individual level, training programs in data science, AI, health informatics, cybersecurity, and data governance are needed to develop the workforce required for health AI systems [24]. Universities and technical institutions across Africa are expanding programs in these areas, but demand far exceeds supply. International partnerships can support capacity building through joint degree programs, short courses, and mentorship, but care must be taken to ensure that training is contextually appropriate and that trained individuals remain in Africa rather than emigrating [24]. Institutional capacity building involves strengthening the ability of healthcare organisations and government agencies to govern health data and AI systems [2]. This includes developing policies and procedures, establishing governance structures, implementing technical infrastructure, and fostering a culture of data stewardship [2]. Technical assistance from international partners can support institutional capacity building, but sustainability requires that institutions develop internal capabilities rather than remaining dependent on external consultants [10].

Ecosystem development involves creating the broader enabling environment for health AI, including regulatory frameworks, research infrastructure, funding mechanisms, and networks for collaboration and knowledge sharing [12]. Regional centres of excellence can serve as hubs for capacity building, research, and technical assistance to multiple countries [24]. South-South collaboration and partnerships among African countries, as well as with other low- and middle-income countries facing similar challenges, can facilitate knowledge transfer and mutual learning [23]. The Africa Data Science Intensive (DSI) program and similar initiatives have demonstrated the potential for building data science capacity across African health institutions through structured training, mentorship, and collaborative research [24]. However, sustaining such initiatives requires long-term commitment and funding.

Capacity building must extend beyond technical skills to include critical perspectives on data governance, ethics, and power dynamics. African professionals need not only to implement AI systems but also to critically evaluate them,

advocate for appropriate governance, and lead the development of contextually appropriate solutions.

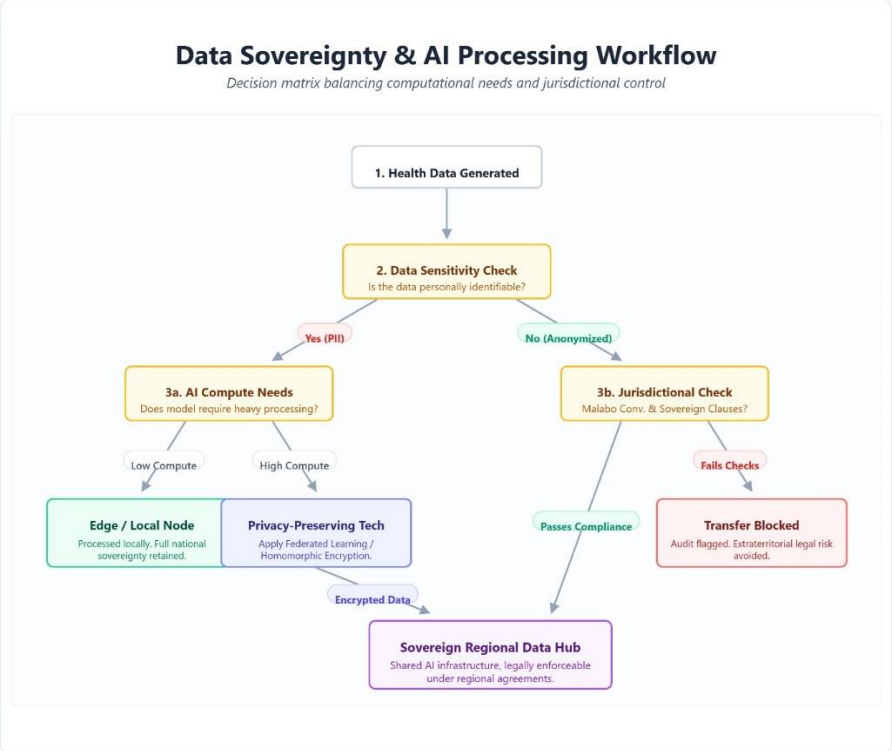
7.5 Auditing and Compliance Technologies.

Sovereignty in the regulation of health data cannot be based solely on statutory prohibition, as it must be operationalised through verifiable enforcement mechanisms. According to Taylor [29], data localisation laws have a normatively strong but institutionally weak nature, as they are not enforced through structures capable of demonstrating adherence. Building on this argument, Prifti et al. [30] argue that governance-by-design should involve control through architectural means rather than arbitrary joins, where the very technical systems become tools of control. Collectively, these views imply that sovereignty cannot be based on such declaratory legal authority. Governments should be in a position to identify the point of data processing, access by third parties and jurisdiction protection. In the absence of these built-in verification mechanisms, there is a likelihood that sovereignty will be merely symbolic and unenforceable.

The data residency verification technologies are thus a basic enforcement layer. In the review of secure health data infrastructures in low- and middle-income settings, Solanke [31] identifies the ability to limit cross-border data breaches through geo-fencing configurations and regional cloud lockdowns. Nevertheless, Yeng et al. [22] warns that technical limitations are ineffective when regulators lack the institutional capacity to conduct an independent compliance audit. They have provided an example of how immutable logging systems and automated audit trails are not sufficiently accompanied by supervisory authorities who can understand and act on such recordings in their work on federated telemedicine governance in Kenya [4]. This synthesis highlights the most important point: technical safeguards are legitimate only when integrated into plausible and effective regulatory ecosystems that can control and penalise deviations.

Encryption control is another Sovereign control, especially in hybrid clouds. Investigating the information systems of Ethiopian hospitals, Denboba et al. [7] contend that states can maintain decisive control, even when information is stored in distributed systems, through national control over encryption keys. Similarly, Yeng et al. [22] shows that federated learning and differential privacy can reduce the flow of raw data, thereby making AI deployment compatible with localisation requirements. However, the digital justice field, as Davis [5] reminds us, depends on choices made in technology design, which cannot be discussed outside power structures. Encryption regimes are not, however, just tools of cybersecurity; they are political decisions concerning who ultimately retains power over sensitive information. In this sense, sovereignty is incorporated into cryptographic architecture to the same extent as it is in legislative texts.

Contractual and procedural compliance mechanisms are also essential beyond their technical enforcement. Michels, Millard, and Turton [32] note that typical cloud service agreements often incorporate arbitration provisions for their foreign operations, circumscribe provider liability, and allow wide-ranging sub-processor contracts, which constrain African bargaining power and are structured to do so. To address these asymmetries, it is not sufficient to aspire to policy solutions; procurement structures must establish audit rights, enforceable deletion guarantees, transparency, reporting requirements, and locally admissible dispute-resolution provisions. Together with third-party certification of independence and regular compliance checks, these tools turn sovereignty, an abstract principle, into a practical reality. Finally, auditing and compliance technologies demonstrate that sovereignty and cloud adoption are not necessarily mutually exclusive; instead, sovereignty should be designed with a layered set of legal, institutional, and computational verification mechanisms.



A Decision Tree or Flowchart illustrating the decision process for data processing. It maps the pathways: "Is data sensitive?" -> "Process Locally/Edge" versus "Is high compute needed?" -> "Transfer to Sovereign Regional Hub with Jurisdictional Clause."

7.6 Economic Pathways to Sovereign Infrastructure

To promote data sovereignty without addressing its economic ramifications is to turn the argument into a sort of normative yearning. The capital-intensive nature of local data centres, comprising the reliability of electricity, cooling systems, cybersecurity measures, and the development of a skilled labour force, in most cases, outweighs the financial means of lower-income states, as Takci et al. [33] note in their evaluation of Ethiopian hospital systems. Similarly, López et al. [10] warn that digital health transformation in a resource-constrained environment should be viewed as competing with urgent healthcare priorities, including workforce expansion and access to medicine. These analyses, taken together, help highlight that sovereignty cannot be conceived as a technical or fiscal choice with significant opportunity costs. The acknowledgement of this fact does not undermine the sovereignty argument but reinforces it, as it prompts policymakers to consider imposing declaratory localisation requirements within long-term economic governance frameworks that can support the long-term establishment of digital independence.

A model of this type is found in the regional data hubs, where infrastructure costs are shared across multiple states without loss of jurisdiction within continental structures. Liaw [34] emphasise the importance of regional economic communities in normalising e-health governance, suggesting that shared digital infrastructure is likely to improve interoperability and regulatory consistency. However, the primary barrier to such regional hubs is not technical but political. Sovereign infrastructure sharing requires a high degree of 'Political Trust' between member states. This trust must be built through the harmonized regulatory standards and 'Multi-Level Governance' outlined in the subsequent sections of this framework. Building on this reasoning, Ivuoma, Chukwuemeka, and Nwadiogbu [35] shows that public-private partnerships between regions in Africa have led to the elimination of duplicative digital investments and enhanced oversight capacity. Instead of having every small state build its own national data centre, sovereign cloud regions at the levels of ECOWAS, SADC, or even the AU would offer shared infrastructure on standards set by the region. This scheme redefines sovereignty as not individual national property, but collective continental property and infrastructure autonomy becomes economically feasible, not by each state funding entire data centre stacks all by itself.

Blended financing and graduated sovereignty also mean completing the reconciliation of fiscal constraint and strategic autonomy. As Masana and Muriithi [14] suggest in South Africa, hybrid architectures enable governments to leverage external cloud capacity and gradually expand in-country hosting capacity. On the same note, Olusanya et al. [16] observe that multilateral partnerships helped drive digital health growth during the COVID-19 response, but long-term sustainability is needed to embed governance safeguards in procurement contracts. Pursuing the national capacity where it is possible and deploying in phases, starting with hybrid implementation and then moving to regional hosting, and finally establishing national capacity, offers a realistic trajectory of transition. The use of edge computing solutions, which enable local data processing at the facility level, can reduce bandwidth costs and reliance on the cloud in the initial phase. When we amalgamate these strategies, we find that economic sovereignty cannot be attained through abrupt isolation but rather through investment strategies in tandem with fiscal realities and institutional preparedness.

8 A FRAMEWORK FOR BALANCING SOVEREIGNTY AND CLOUD-BASED AI

8.1 Principles for Governance-by-Design

Effective governance of African health AI requires embedding principles of sovereignty, privacy, equity, and accountability into systems from the design stage rather than retrofitting governance onto existing systems [16, 36]. This "governance-by-design" approach recognises that technical architectures embody governance choices and that early design decisions can enable or constrain future governance options [36].

This paper proposes seven core principles for governance-by-design in African health AI:

1. Data Sovereignty by Default

Data Sovereignty by Default requires that system architectures embed jurisdictional control as the baseline condition rather than as an afterthought [19]. This principle moves beyond symbolic localisation mandates by demanding that technical configurations, such as geo-fencing, region-locked cloud deployment, and national custody of encryption keys, ensure that data remain within authorised jurisdictions unless explicit regulatory approval permits transfer. By making sovereignty the architectural default, governments reduce reliance on post hoc enforcement and contractual assurances. Cross-border transfers should therefore be conditional, documented, and auditable, rather than operationally seamless. In this model, sovereignty is not achieved through isolation but through deliberate design choices that preserve national and regional authority while allowing calibrated participation in global digital ecosystems.

2. Privacy Preservation

Privacy Preservation requires that health AI systems integrate data protection safeguards into their design rather than relying on reactive compliance measures. Data minimisation, end-to-end encryption, role-based access controls, and immutable audit logs must be embedded as structural components of digital infrastructure. Privacy-enhancing technologies such as differential privacy and federated learning further limit unnecessary exposure of identifiable information while preserving analytical utility. By integrating these mechanisms into system architecture, regulators shift from enforcement-driven compliance to preventive governance. Privacy thus becomes a continuous operational feature rather than a legal abstraction. In the African health context, where regulatory capacity may be uneven, embedding privacy into design reduces vulnerability and strengthens institutional resilience against misuse or unauthorised access

3. Transparency and Explainability

Transparency and Explainability require that AI systems deployed in clinical environments provide intelligible reasoning for their outputs to clinicians, regulators, and affected patients. In high-stakes healthcare decisions, opaque “black-box” models undermine both clinical trust and regulatory oversight. Systems should therefore include interpretable model components, traceable decision pathways, and documentation of the provenance of training data. Where complex models are unavoidable, post hoc explanation tools must provide meaningful insights into the rationale for the output. Transparency also extends to governance processes, including disclosure of algorithm updates and performance audits.

4. Equity and Inclusion

Equity and Inclusion require that health AI systems support the needs of diverse populations without exacerbating existing inequalities. Performance based on algorithms should be measured across demographic groups to avoid bias associated with ethnicity, geography, language, or socioeconomic status. Inclusive design demands multilingual interfaces, culturally appropriate communication tools, and other accessibility features that support different levels of literacy and technological access. The approaches to data collection must focus on the representation of historically marginalised communities in order to prevent biased model results. Equity is thus not just about metrics of fairness but about structural inclusion in system design and in its governance. Considering the heterogeneity of African contexts in terms of health and digital access, integrating equity protections ensures that technological innovation promotes, rather than reinforces, existing inequalities.

5. Local Control and Flexibility

Local Control and Flexibility is a way to ensure that national health authorities and institutional administrators have significant decision-making power over digital systems. This principle avoids fixed vendor architectures that limit configuration, data portability, or interoperability. Governments can customise systems to current regulatory needs using open standards, modular system design, and transparent APIs, without overreliance on proprietary platforms. The need to avoid vendor lock-in is especially important when fiscal constraints reduce the leverage to renegotiate. Local control also includes data access policies, model deployment thresholds, and procurement. States can retain strategic independence by introducing flexibility into procurement systems and structures and remaining compatible with regional and global health ecosystems.

6. Accountability and Redress

Accountability and Redress require clearly defined investigative authority, jurisdictional clarity, and enforceable remedies when health data are breached, misused, or transferred unlawfully. In cases of violation, independent national data protection authorities must be empowered to initiate investigations, compel disclosure of audit logs, and impose administrative sanctions on both domestic and foreign cloud providers operating within the jurisdiction. Crucially, this must be enforced through 'Jurisdictional Clauses' in cloud procurement contracts. These clauses must mandate that legal disputes are settled in African courts under local laws, preventing foreign providers from hiding behind extraterritorial legal shields. Regulatory frameworks should require foreign providers to establish a legal presence or designated representative in-country, ensuring that local courts retain jurisdiction over disputes. Citizens must have the right to file complaints directly with supervisory authorities and pursue civil action in domestic courts where harm has occurred. Without such locally enforceable pathways, sovereignty lacks practical meaning.

Redress mechanisms must also include proportional financial penalties, rights to compensation, and contractual safeguards embedded in procurement agreements. Arbitration clauses that displace domestic jurisdiction to foreign courts should be restricted or subject to mutual recognition frameworks under regional instruments such as the Malabo Convention. Regulatory fines must be calibrated to deter non-compliance, including the authority to suspend or terminate operating licences for repeated violations. At the regional level, coordinated oversight mechanisms can facilitate cross-border enforcement where data transfers occur under harmonised agreements. Technical systems should maintain immutable audit trails to support evidentiary proceedings. Through layered legal, institutional, and technical enforcement, accountability becomes an operational defence rather than a symbolic assurance.

Systems should be designed with long-term sustainability in mind, including consideration of ongoing costs, maintenance requirements, and capacity building needs. Dependency on external actors should be minimised. These principles should guide procurement decisions, system design, and policy development. Governance frameworks should include mechanisms to assess whether systems comply with these principles and to hold vendors and implementers accountable.

8.2 Multi-Level Governance Architecture

Effective governance of African health AI requires coordination across multiple levels: individual healthcare facilities, national governments, regional economic communities, and continental bodies [2]. A multi-level governance architecture is proposed that specifies roles and responsibilities at each level while enabling coordination and harmonisation. The figure below is a Pyramidal or Nested Circle Diagram showing the flow of data and authority from the Facility Level (base) up to the Continental Level (peak). It includes arrows to show "Data Flows" pointing upward and "Policy/Governance Standards" pointing downward.

Multi-Level Governance Architecture

8.2.1 Facility Level

Individual healthcare facilities are responsible for implementing data protection practices, ensuring informed consent, managing access controls, and monitoring the performance of AI systems in clinical practice. Facilities should have designated data protection officers and ethics committees to oversee the use of health AI.

8.2.2 National Level

National governments are responsible for establishing legal and regulatory frameworks for health data protection and AI governance, developing national health information infrastructure, setting interoperability and data-quality standards, and overseeing public- and private-sector health AI implementations. National data protection authorities should have adequate resources and authority to enforce regulations.

8.2.3 Regional Level

Regional economic communities should harmonise data protection laws and AI governance frameworks across member states, facilitate cross-border data sharing for legitimate purposes under appropriate safeguards, coordinate capacity-building initiatives, and establish regional centres of excellence for health AI.

8.2.4 Continental Level

The African Union and pan-African bodies should develop continent-wide frameworks and principles for health data governance and AI, facilitate knowledge sharing and best practice dissemination, coordinate with international partners on behalf of African interests, and advocate for equitable participation in global AI governance.

Coordination mechanisms are needed to ensure coherence across levels. National policies should align with regional frameworks, which, in turn, must correspond to continental principles. Regular stakeholder dialogue forums at different levels can facilitate coordination. Technical standards for

interoperability and data exchange should be harmonised to enable cross-border collaboration while maintaining sovereignty. This multi-level architecture recognises that different governance functions are best performed at different levels. Detailed implementation decisions are best made locally, where context-specific knowledge is greatest. Harmonisation and coordination are best achieved at the regional and continental levels. The architecture should be sufficiently flexible to accommodate the diversity of African contexts while providing sufficient coordination to enable effective collaboration.

9 DISCUSSION

9.1 Implications for Policy and Practice

This analysis has several important implications for policymakers, healthcare institutions, technology providers, and civil society organisations working on African health AI governance. The trajectory of African digital health can be visualized as a 'Sovereignty-Innovation Curve.' In the early phase, states act as passive data sources for international platforms. As nations adopt the hybrid models and regional hubs suggested here, they move along the curve toward becoming independent innovators who use sovereign data to build locally-relevant AI.

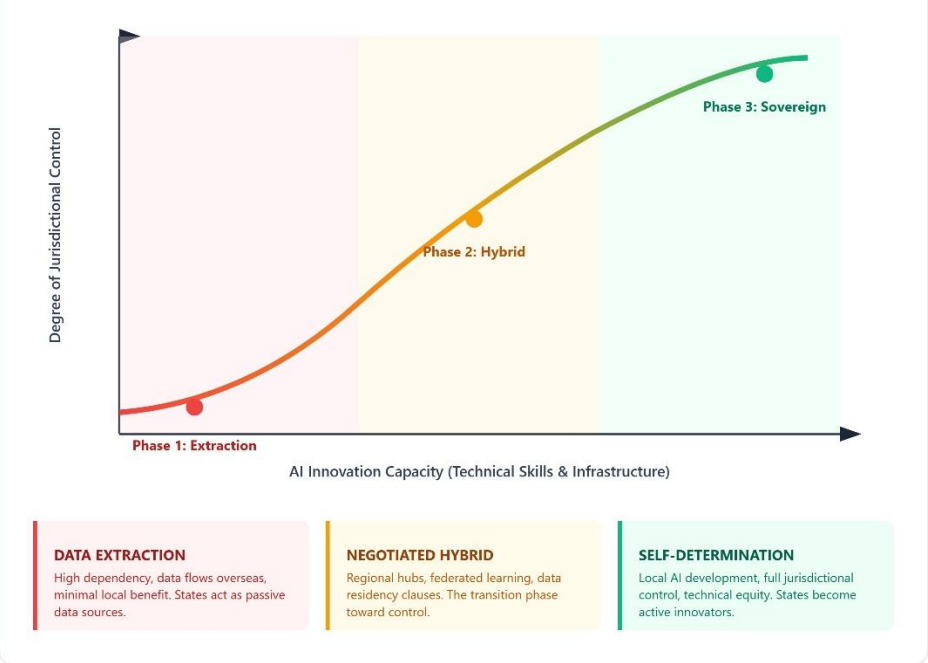


Fig 1: Source: Sanchez (2024) https://veridas.com/en/what-is-zero-trust/

If necessary, the images can be extended both columns

9.1.1 Policymakers

Data sovereignty and cloud-based AI are not inherently incompatible, but achieving both requires deliberate governance design. Policymakers should avoid binary choices between strict data localisation and unrestricted cloud adoption, instead pursuing hybrid approaches that maintain sovereignty while enabling beneficial innovation. Moreover, regional harmonisation of data protection laws and AI governance frameworks should be prioritised to facilitate cross-border collaboration while maintaining protection standards. Lastly, investments in infrastructure and capacity building are essential prerequisites for effective governance and should be treated as health system priorities, not merely technology projects.

9.1.2 Healthcare Institutions

Institutions implementing health AI systems should conduct thorough due diligence on vendors and cloud providers, ensuring that contracts include explicit sovereignty protections, data protection requirements, and provisions for local control. Additionally, governance structures, including data protection officers, ethics committees, and community advisory boards, should be established before deploying AI systems, not as afterthoughts. Lastly, staff training in data governance and AI ethics should be prioritised alongside technical training.

9.1.3 Technology Providers

Companies providing cloud services and AI tools to African healthcare systems should recognise that extractive practices and one-size-fits-all solutions are neither ethical nor sustainable. Providers should offer flexible deployment options, including local hosting, hybrid architectures, and privacy-preserving technologies. Also, transparent pricing, open standards, and avoidance of vendor lock-in should be standard practices. Mostly, meaningful capacity building and technology transfer should be integrated into partnerships rather than treated as optional add-ons.

9.1.4 Civil Society Organisations

Civil society has critical roles in advocating for rights-based data governance, monitoring the implementation of governance frameworks, and facilitating community participation in decision-making. Organisations should work to build public understanding of health AI governance issues and to amplify community voices in policy processes. Lastly, holding governments and corporations accountable for governance commitments requires sustained civil society engagement.

9.1.5 International Partners

Development partners, research institutions, and multilateral organisations should align their support with African priorities and governance frameworks rather than imposing external models. Partnerships should be structured to build African capacity and ownership rather than creating dependencies.

Additionally, funding should support long-term governance infrastructure, not just short-term technology deployments.

The COVID-19 pandemic demonstrated both the potential and the risks of rapid digital health adoption without adequate governance. As African countries continue to invest in health AI, the decisions made now will shape the continent's health systems for decades. Getting governance right is not a luxury or an obstacle to innovation; it is a prerequisite for sustainable, equitable, and trustworthy health AI.

9.2 Limitations and Future Research Directions

This analysis has several limitations that should be acknowledged. First, the evidence base on African health AI governance is still developing. While we identified substantial literature on digital health, data governance, and AI in African contexts, empirical studies of implemented governance frameworks and their impacts remain limited. Many of the case studies discussed are recent initiatives whose long-term outcomes are not yet clear. Second, the diversity of African contexts means that generalisations are necessarily limited. Governance challenges and appropriate solutions vary significantly across countries with different levels of development, regulatory capacity, infrastructure, and political systems.

The proposed framework attempts to be flexible and adaptable, but implementation will require substantial contextualization. Third, the rapid pace of technological change requires governance frameworks to be dynamic and adaptive. Technologies such as large language models, edge AI, and quantum computing may create new governance challenges that current frameworks do not adequately address. Governance systems must include mechanisms for ongoing learning and adaptation. Fourth, this analysis has focused primarily on technical and regulatory dimensions of governance, with less attention to political economy factors. Power dynamics, vested interests, and political will significantly influence governance outcomes but are difficult to analyse systematically. Future research should examine the political economy of health AI governance in greater depth.

Several important directions for future research emerge from this analysis:

i. Rigorous studies of implemented governance frameworks, examining their effectiveness, costs, unintended consequences, and impacts on health outcomes, equity, and innovation.
ii. Research on the feasibility, performance, and cost-effectiveness of federated learning, differential privacy, and other privacy-preserving technologies in resource-constrained settings.
iii. Qualitative research exploring how African communities understand and value data sovereignty, privacy, and AI in healthcare, and how governance frameworks can better reflect community priorities.
iv. Cost-benefit analyses of different governance approaches, including infrastructure investments, regulatory compliance costs, and opportunity costs of various sovereignty-cloud trade-offs.
v. Systematic comparison of governance approaches across countries, identifying factors associated with successful implementation and lessons for policy transfer.
vi. Research on how health AI governance intersects with broader digital governance, trade policy, intellectual property regimes, and development strategies.
vii. Studies examining the sustainability of governance frameworks over time, including financing mechanisms, capacity retention, and adaptation to technological change.

Addressing these research gaps will require sustained investment in African health policy and systems research capacity, as well as genuine partnerships between African and international researchers that respect African leadership and priorities.

10 CONCLUSION

Governance of health AI in Africa is not only a regulatory issue, but also a structural paradigm shift in the digital path of the continent. Cloud computing and artificial intelligence are potentially transformative-they will improve and make diagnostic processes better and more precise, create predictive analytics of public health, and expand scarce medical resources by providing scalable infrastructure. However, these advantages cannot be independent of the governance decisions that define data ownership, the beneficiary of the data, and the jurisdiction under which authority is exercised. In this paper, it has been established that there is no binary opposition between data sovereignty and cloud dependency and that an institutional and technical response is necessary in the design. This terrain is complicated by fragmented regulatory regimes, infrastructural inequalities, imbalanced bargaining power, and threats of digital colonialism. Nevertheless, these limitations do not rule out innovation; instead, they require a governance design that can convert sovereignty in principle to enforceable practice.

Reinterpreting trade-offs as a Conflict-Resolution Framework shows that sovereignty and innovation may be harmonised through layered instruments. Privacy-preserving technologies, federated learning architectures, regionally harmonised transfer agreements, and hybrid cloud deployments all indicate that regulatory surrender is not necessary to advance technology. The coordination of multi-level governance, which spans healthcare facilities, national regulators, regional bodies, and continental institutions, is important so that enforcement mechanisms act in a coherent manner and not in isolation from one another. Most importantly, this architecture is supported by accountability and redress mechanisms that provide citizens with a remedy in cases of misuse or infringement. When there is convergence among legal authority, technical verification, and institutional capacity, then sovereignty becomes operational. Governance maturity does not come with isolationism but is facilitated by organised integration that safeguards jurisdiction and enables participation in global AI ecosystems.

This can be theorised as a Sovereignty-Innovation Curve. In its first phase, African states are treated as data sources and provide valuable health data to international platforms, without control over infrastructure or model development. Defensive localisation policies are reactive claims of power but can limit computational capacity when pursued independently. The regional data hubs and gradual infrastructure investment support the transition to calibrated hybrid governance, enabling progress towards independence in innovation. On top of this curve, African institutions use sovereign data to build context-specific AI systems based on local epidemiological data. Sovereignty is therefore transformed from a defensive stance to a generative platform of technological self-determination. Whether Africa will enter the global AI economy is not the question; rather, it is whether it will be a passive data producer or an independent innovator.

The further development relies on long-term political commitment, institutional alignment, and long-term investments. Governments should focus on enforcing data governance schemes and developing regulatory capacities to

regulate intricate digital ecosystems. The regional collaboration would be able to share infrastructure costs and leverage its bargaining power in negotiations with multinationals in the technology industry. Public-private partnerships need to incorporate the corpus of sovereignty, capacity-building and clauses of equitable benefit-sharing. Civil society participation is still necessary to maintain legitimacy and secure rights. Making African states replaced by data extraction zones to AI-generating ecosystems does not come automatically or as a given but involves purposeful governance design in line with continental priorities. African countries can strategically reestablish digital governance worldwide by showing that innovation and sovereignty are not in opposition but support each other as pillars of technological justice.

11. ACKNOWLEDGMENTS

I express my sincere gratitude to the experts, mentors, and peers who have significantly contributed to the development of this research paper. Their insights, guidance, and support were invaluable in shaping this work.

12 REFERENCES

[1] M. A. Oladosu et al., "Exploring Digital Health Innovations Across Africa: Challenges, Opportunities and the Way Forward," Journal of Health Informatics in Africa, vol. 12, no. 2, pp. 47-68, 2026.

[2] F. S. Sidii, "Building Trust and Sovereignty: A Holistic Framework for Data Governance in African Healthcare Systems," Health Economics and Management Review, vol. 6, no. 3, pp. 56-74, 2025.

[3] R. Prasad et al., "Transforming African Healthcare with AI-Driven Data Analytics and Predictive Medicine for Sustainable and Inclusive Health Outcomes," in Sustainable Healthcare Systems in Africa, pp. 215-233, 2025.

[4] N. Tiffin, A. George, and A. E. LeFevre, "How to use relevant data for maximal benefit with minimal risk: Digital health data governance to protect vulnerable populations in low-income and middle-income countries," BMJ Global Health, vol. 4, no. 2, p. e001395, 2019.

[5] S. L. M. Davis, "Towards digital justice: Participatory action research in global digital health," BMJ Global Health, vol. 7, no. 5, p. e009351, 2022.

[6] S. Calzati, "'Data sovereignty' or 'Data colonialism'? Exploring the Chinese involvement in Africa's ICTs: A document review on Kenya," Journal of Contemporary African Studies, vol. 40, no. 2, pp. 270-285, 2022.

[7] W. Denboba et al., "Strengthening Ethiopia's Health Information System: A Journey to Unified DHIS2," Ethiopian Journal of Health Development, vol. 38, no. 2, pp. 1-6, 2024.

[8] B. Ogwel, G. Odhiambo-Otieno, G. Otieno, J. Abila, and R. Omore, "Leveraging cloud computing for improved health service delivery: Findings from public health facilities in Kisumu County, Western Kenya," Learning Health Systems, vol. 5, no. 2, 2021.

[9] P. Apiko and M. Musoni, "Realising the potential of AI for diagnostics in Africa: From barriers to scalability," ECDPM Discussion Paper, 2025.

[10] D. M. López, C. Rico-Olarte, B. Blobel, and C. Hullin, "Challenges and solutions for transforming health ecosystems in low- and middle-income countries through artificial intelligence," Frontiers in Medicine, vol. 9, 2022.

[11] K. S. Adewole et al., "A systematic review and meta-data analysis of clinical data repositories in Africa and beyond: Recent development, challenges, and future directions," Discover Data, vol. 2, no. 1, 2024.

[12] U. Tanveer, T. G. Hoang, S. Ishaq, and R. U. Khalid, "Public-private partnerships as catalysts for digital transformation and circular economy: Insights from developing countries," Technological Forecasting and Social Change, vol. 219, p. 124270, 2025.

[13] N. Masana, "State of medical record systems and the adoption of cloud-based medical record systems in public healthcare facilities in Free State," International Conference on Emerging Technology and Interdisciplinary Sciences, vol. 2, no. 3, pp. 9-19, 2022.

[14] N. Masana and G. M. Muriithi, "Adoption of an Integrated Cloud-Based Electronic Medical Record System at Public Healthcare Facilities in Free-State, South Africa," in Proceedings of the Conference on Information Communications Technology and Society (ICTAS), pp. 1-6, 2019.

[15] J. K.-K. Zao et al., "Design of a Trustworthy Cloud-Native National Digital Health Information Infrastructure for Secure Data Management and Use," Oxford Open Digital Health, vol. 2, no. 4, 2024.

[16] O. A. Olusanya, B. White, C. A. Melton, and A. Shaban-Nejad, "Examining the Implementation of Digital Health to Strengthen COVID-19 Pandemic Response and Recovery and Scale up Equitable Vaccine Access in African Countries," JMIR Formative Research, vol. 6, no. 5, 2022.

[17] M. van Reisen et al., "Design of a FAIR digital data health infrastructure in Africa for COVID-19 reporting and research," Advanced Genetics, vol. 2, no. 2, 2021.

[18] S. Sahu, N. Mallick, and K. Garikapati, "The Intersection of Digital Health and Data Privacy: A Legal Perspective," in Sustainable Healthcare Systems in Africa, pp. 187-214, 2025.

[19] W. P. dos Santos et al., "Nations of the Global South: Pioneering the Future of Health with Artificial Intelligence and Digital Health Sovereignty," Artificial Intelligence and Bioethics, vol. 14, no. 2, pp. 48-65, 2025.

[20] A. Owoyemi et al., "Trustworthy AI in Healthcare: Exploring Ethics in Digital Health Technologies in Nigeria," in Trustworthy AI, vol. 8, no. 3, pp. 193-206, 2025.

[21] A. I. Oladimeji, A. A. Jimoh, and Y. A. Huussaini, "Computing Innovation for Healthcare Delivery in the Intelligent Age: Pathways to Inclusive and Sustainable Development," International Journal of Science Research and Technology, vol. 5, no. 3, 2025.

[22] P. K. Yeng et al., "HEALER2: A Framework for Secure Data Lake Towards Healthcare Digital Transformation Efforts in Low and Middle-Income Countries," in Proceedings of IEEE, pp. 31-39, 2023.

[23] R. Rayan, "Ehealth opportunities for the low and middle-income countries," Global Journal of Public Health Medicine, vol. 2, no. 1, pp. 158-163, 2020.

[24] A. N. Kiragga et al., "Data science without borders: Bridging the divide in data science capacity across African health institutions," Frontiers in Public Health, vol. 13, 2025.

[25] M. T. T. Bajwa et al., "Cloud-Native Architectures for Large-Scale AI-based Predictive Modeling," Journal of Emerging Technology and Digital Transformation, vol. 4, no. 2, pp. 207-221, 2025.

[26] D. Denyer and D. Tranfield, "Producing a systematic review," in The Sage Handbook of Organizational Research Methods, pp. 671-689, 2009.

[27] S. Naidoo et al., "Artificial intelligence in healthcare: Proposals for policy development in South Africa," South African Journal of Bioethics and Law, vol. 15, no. 1, pp. 11-16, 2022.

[28] African Union Commission, African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), Addis Ababa, 2024.

[29] R. D. Taylor, "'Data localization': The internet in the balance," Telecommunications Policy, vol. 44, no. 8, p. 102003, 2020.

[30] K. Prifti, J. Morley, C. Novelli, and L. Floridi, "Regulation by Design: Features, Practices, Limitations, and Governance Implications," Minds and Machines, vol. 34, no. 2, 2024.

[31] A. A. Solanke, "Sovereign cloud implementation: Technical architectures for data residency and regulatory compliance," International Journal of Science and Research Archive, vol. 11, no. 2, pp. 2136-2147, 2024.

[32] J. D. Michels, C. Millard, and F. Turton, "Standard Contracts for Cloud Services," Cloud Computing Law, vol. 5, no. 1, pp. 49-99, 2021.

[33] M. T. Takci, M. Qadrdan, J. Summers, and J. Gustafsson, "Data centres as a source of flexibility for power systems," Energy Reports, vol. 13, pp. 3661-3671, 2025.

[34] S.-T. Liaw, J. Jonnagaddala, M. A. Godinho, and Y. Wilkins-Wong, Digital Health Maturity: Quality, Interoperability, and Innovation. Academic Press, 2025.

[35] D. Ivuoma, E. Chukwuemeka, and N. Nwadiogbu, "Government Interference in Public Business in Nigeria: Problems and Prospects," Journal of Policy and Development Studies, vol. 19, no. 1, pp. 104-122, 2025.

[36] B. A. Townsend, "Governance-by-Design as an Enabler of AI in Digital Health in Sub-Saharan Africa," Law, Technology and Humans, vol. 8, no. 3, 2025.