

Integrating Digital Health into Weak Governance Systems: A Policy Framework for Health System Strengthening in Sub-Saharan Africa

Alplato Chukpue-Padmore

chukpuepadmore2019@gmail.com

Center For Integrated Solutions

Emmanuel Flomo

Center For Integrated Solutions

Research Article

Keywords: digital health, health system strengthening, weak governance, cybersecurity, Sub-Saharan Africa, health policy, interoperability, digital health governance

Posted Date: October 6th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11245455/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

Background

Sub-Saharan Africa (SSA) carries a disproportionate share of the global disease burden while operating within severely resource-constrained health systems. Although digital health technologies, including mobile health (mHealth), electronic health records (EHRs), and telemedicine, offer genuine transformative potential, their integration is routinely undermined by weak governance structures, fragmented policy frameworks, and inadequate cybersecurity infrastructure.

Methods

This study employed qualitative policy analysis and narrative synthesis of secondary data. Quantitative indicators on health outcomes, digital infrastructure, and governance were drawn from the World Health Organization (WHO), the World Bank Worldwide Governance Indicators, UNICEF, and the GSMA. A systematic review of peer-reviewed literature and national digital health strategic plans identified structural barriers to adoption.

Results

Digital health initiatives in SSA are characterized by "pilotitis," a proliferation of donor-funded, fragmented, and non-interoperable pilot projects. Key barriers include infrastructural deficits (only 22% of health facilities have reliable internet access), weak regulatory frameworks, and an acute cybersecurity gap, with African healthcare organizations facing an average of 3,575 weekly cyberattacks. The estimated digital health funding shortfall for Africa is approximately USD 4.1 billion for the period 2024 to 2030.

Conclusions

Digital health interventions introduced without governance reform reproduce and amplify existing health system failures. Sustainable integration requires a paradigm shift from technology-centric deployment to governance-centric integration. We propose the Digital Health Governance Integration Model (DHGIM), a policy framework emphasizing structural alignment, regulatory fortification, and institutional capacity absorption as the foundational pillars for resilient, equitable digital health systems in fragile governance environments.

Introduction

Sub-Saharan Africa (SSA) faces a dual challenge: it carries the highest global burden of disease while operating with some of the most resource-constrained and fragile health systems anywhere in the world

[2]. The region accounts for approximately 70% of global maternal deaths and has an under-five mortality rate of 72 per 1,000 live births, significantly higher than the global average [1,2]. In response to these persistent challenges, digital health technologies, encompassing mobile health (mHealth), electronic health records (EHRs), telemedicine, and health management information systems (HMIS), have emerged as critical tools for health system strengthening [3]. The African digital health market, valued at approximately USD 3.8 billion in 2023, is projected to grow at a compound annual growth rate (CAGR) of 23.4%, reaching USD 16.6 billion by 2030 [4]. These projections are drawn from commercial market analysis and should be interpreted as indicative estimates; they are cited here to contextualize the scale of investment interest rather than as independently verified research findings.

Despite this rapid technological expansion, translating digital innovation into sustained health outcomes remains inconsistent across the continent. The primary impediment is not the availability of technology, but the weakness of the governance systems into which these technologies are introduced [5]. In many SSA countries, digital health initiatives are characterized by "pilotitis," a proliferation of donor-funded, fragmented, and non-interoperable pilot projects that fail to scale nationally [6]. This fragmentation is compounded by weak regulatory frameworks, inadequate cybersecurity infrastructure, and a lack of institutional capacity to manage complex digital transformations [7].

The theoretical foundation for digital health in low- and middle-income countries (LMICs) rests on its potential to bypass traditional infrastructural deficits, a phenomenon often described as "technological leapfrogging" [8]. High mobile phone penetration in SSA, which reached 51% in 2023, has facilitated the widespread adoption of mHealth interventions for disease surveillance, maternal health tracking, and supply chain management [9]. Research has shown that digital health can enhance healthcare delivery in underserved areas by enabling remote care, improving diagnostic accuracy, and optimizing resource allocation [10].

However, the reality of digital health implementation often falls short of its promise. A systematic review of national digital health strategic plans in Africa revealed significant weaknesses in contextualization, intervention focus, and technological foresight [6]. Of the 54 African nations, while many have adopted digital health strategies, these plans frequently lack alignment with actual health system challenges, adequate funding mechanisms, and provisions for emerging technologies such as artificial intelligence [6].

Governance quality is a fundamental determinant of health system performance. The World Bank's Worldwide Governance Indicators (WGI), which measure government effectiveness, regulatory quality, rule of law, and control of corruption, consistently show a strong correlation between good governance and improved health outcomes [11]. In West Africa, empirical evidence demonstrates that enhancing governance dimensions significantly reduces infant and maternal mortality rates and improves life expectancy [12]. Conversely, weak governance manifests in the health sector through inefficient resource allocation, lack of accountability, and the inability to enforce regulations [12]. When digital health

systems are introduced into such environments, they often inherit and amplify these systemic weaknesses.

This paper argues that digital health interventions introduced without governance reform systematically reproduce and amplify existing health system failures. The successful integration of digital health in Sub-Saharan Africa requires governance reform to precede, not follow, technology deployment. We propose the Digital Health Governance Integration Model (DHGIM), a three-pillar policy framework that positions structural alignment, regulatory fortification, and institutional capacity absorption as the foundational conditions for resilient and equitable digital health systems in fragile governance environments.

Literature Review

The scholarly literature on digital health in low- and middle-income countries has grown substantially over the past decade, yet it remains characterized by a persistent tension between technological optimism and governance realism. Early scholarship, shaped largely by the enthusiasm surrounding mobile phone proliferation in Africa, emphasized the transformative potential of mHealth to leapfrog traditional infrastructural deficits [8]. More recent work, however, has begun to interrogate the structural conditions under which digital health interventions either succeed or fail, shifting the analytical lens from technology to the institutional environments that receive it.

Digital Health Adoption and the Leapfrogging Hypothesis

The concept of technological leapfrogging - the idea that developing regions can bypass intermediate stages of infrastructure development by adopting advanced technologies directly- has been a central organizing theme in the digital health literature [8]. The rapid expansion of mobile connectivity across SSA lent credibility to this thesis. By 2023, mobile penetration had reached 51% across the continent, and mHealth applications had demonstrated measurable impact in areas ranging from maternal health tracking to supply chain management and disease surveillance [9]. Studies conducted in Kenya, Rwanda, and Nigeria documented improvements in antenatal care attendance, medication adherence, and community health worker performance following the introduction of mobile-based health information systems [13,14].

Nonetheless, the leapfrogging hypothesis has faced sustained critique. Scholars have noted that mobile penetration statistics often obscure significant disparities in device quality, data affordability, and digital literacy, particularly among rural and low-income populations [10]. Furthermore, the assumption that connectivity alone is sufficient to drive health system improvement neglects the organizational and regulatory conditions necessary for digital tools to function at scale. As Dugani [5] observed, the digitalization of health care in LMICs frequently stalls not because of technological limitations, but because the institutional infrastructure required to govern, maintain, and adapt these systems is absent.

Governance Deficits and the "Pilotitis" Problem

A recurring theme in the literature is the phenomenon of "pilotitis," a term coined to describe the proliferation of small-scale, donor-funded digital health projects that operate in isolation from national health systems and from one another [6]. Systematic reviews of national digital health strategic plans across Africa have found that the majority of such plans lack coherent interoperability standards, sustainable financing mechanisms, and provisions for scaling successful pilots into national programs [6]. The result is a fragmented landscape of parallel systems, each serving a narrow programmatic objective while collectively undermining the coherence of the national health information architecture [7].

The governance literature offers a useful framework for understanding why this pattern persists. The World Bank's Worldwide Governance Indicators consistently demonstrate that countries with lower scores on government effectiveness, regulatory quality, and rule of law are significantly less likely to achieve successful digital health integration [11]. Kouadio [12] found that in West African countries, improvements in governance quality were among the strongest predictors of reductions in infant and maternal mortality, suggesting that governance reform and health system strengthening are inseparable objectives. Greer et al. [22] similarly argued that health system governance, encompassing the rules, norms, and accountability mechanisms that shape how health systems operate, is the foundational determinant of whether any health intervention, digital or otherwise, can be sustained over time.

Donor dependency compounds these governance deficits. Because digital health initiatives in SSA are disproportionately funded by external actors operating on short project cycles, they are rarely designed with national ownership or long-term institutional integration in mind [7]. When funding cycles end, the systems they created frequently collapse, leaving behind fragmented data, trained staff who have moved on, and communities that have lost access to services they had come to rely on. Transform Health Coalition [24] estimated that closing the digital health funding gap in Africa, projected at USD 4.1 billion between 2024 and 2030, will require a fundamental shift from donor-driven project financing to domestically integrated health budgets.

Cybersecurity as a Governance Imperative

One of the most significant gaps in the existing digital health literature is its treatment of cybersecurity as a peripheral technical concern rather than a core governance issue. As health systems across SSA have digitized patient records, deployed connected medical devices, and expanded telemedicine networks, the attack surface available to malicious actors has expanded dramatically. Industry threat intelligence data indicate that healthcare organizations in Africa face an average of 3,575 cyberattacks per week, more than double the global average [15]. While this figure derives from commercial threat intelligence reporting rather than peer-reviewed research, the underlying pattern it describes, namely an acute and growing cybersecurity exposure in African health systems, is corroborated by independent regulatory analyses and policy reviews [16,10]. The threat landscape is dominated by phishing attacks (38%), ransomware (27%), and data breaches targeting electronic medical records (18%), with state-sponsored actors increasingly targeting health data for geopolitical purposes [17].

The regulatory environment compounds this vulnerability. McKay and Mwangi [16] conducted a comparative analysis of health data regulation across African jurisdictions and found that while many countries have enacted broad data protection legislation, very few have developed health-sector-specific cybersecurity standards or enforcement mechanisms. The result is a regulatory vacuum in which digital health vendors operate with minimal accountability for the security of the systems they deploy. The National Institute of Standards and Technology (NIST) [18] Cybersecurity Framework 2.0 provides a widely adopted baseline standard, but its adoption in African health ministries remains limited, partly because of capacity constraints and partly because procurement processes rarely include security as a mandatory evaluation criterion [17].

The intersection of weak governance and poor cybersecurity infrastructure creates a particularly dangerous environment. In contexts where accountability mechanisms are weak, data breaches may go unreported, affected patients may have no legal recourse, and systemic vulnerabilities may persist for years without remediation. Segun-Omosehin et al. [10] argued that the failure to treat cybersecurity as a governance imperative, rather than an IT afterthought, represents one of the most consequential policy gaps in the current digital health landscape across SSA.

Toward a Governance-Centered Framework

Several scholars have called for a reorientation of the digital health literature away from technology-centric frameworks and toward approaches that foreground governance, institutional capacity, and political economy [5,7]. The WHO/ITU National eHealth Strategy Toolkit and the Smart Africa Digital Health Blueprint [21] represent important steps in this direction, providing guidance on national strategy development, interoperability standards, and stakeholder coordination. However, these frameworks have been criticized for underestimating the depth of governance reform required in fragile state contexts and for providing insufficient guidance on cybersecurity integration [6].

This paper builds on and extends these contributions by proposing the Digital Health Governance Integration Model (DHGIM), a framework designed specifically for weak governance environments. Unlike existing approaches that treat governance as one component among many, the DHGIM positions governance reform as the necessary precondition for any sustainable digital health integration. It integrates cybersecurity as a structural pillar rather than an add-on, and it provides a phased implementation roadmap that acknowledges the real constraints facing health ministries in resource-limited settings.

Methods

This research employs directed content analysis and narrative synthesis of secondary data to construct a comprehensive understanding of digital health governance in Sub-Saharan Africa. Directed content analysis was chosen because the study begins with an established theoretical framework, specifically the WHO Health System Building Blocks and the TAPIC governance dimensions, and uses this

framework to systematically code and interpret evidence from the literature regarding barriers to digital health integration. This approach is appropriate for policy framework development, as it allows existing theory to guide analysis while remaining open to emergent themes not anticipated by the initial framework [19].

Data Collection

Data on health outcomes, digital infrastructure, and governance indicators were sourced from the WHO Global Health Observatory, the World Bank DataBank (Worldwide Governance Indicators), UNICEF, and the GSMA Mobile Economy reports covering 2023 and 2024. Cybersecurity threat data in African healthcare were drawn from the Microsoft Threat Intelligence Report [15] and industry analyses by Digital Health Africa [17]. As commercial and advocacy sources, these are used to contextualize the scale of cybersecurity exposure; their findings are treated as indicative rather than definitive, and are corroborated where possible with peer-reviewed regulatory analyses.

Literature Synthesis

We conducted a systematic review of peer-reviewed literature, policy briefs, and national digital health strategic plans across four search domains: digital health governance, health system strengthening, cybersecurity in African healthcare, and digital health policy frameworks. The review focused on identifying the structural barriers to digital health implementation and the impact of governance quality on health system performance in LMICs.

Framework Development

The proposed policy framework was developed by synthesizing the WHO/ITU National eHealth Strategy Toolkit, the TAPIC governance framework, and established cybersecurity management principles. TAPIC is an acronym for Transparency, Accountability, Participation, Integrity, and Capacity – five dimensions of governance quality that the framework uses to assess the institutional conditions under which health policy can be effectively designed, implemented, and sustained [22]. Integrating TAPIC into the DHGIM allows the framework to evaluate not just what digital health policies say, but whether the governance environment is capable of making them work. The framework was designed to address the specific vulnerabilities identified in the literature review and data analysis, providing actionable recommendations for policymakers in weak governance environments.

Results

Health Burden and Governance Deficits

The analysis of health burden indicators confirms stark disparities between Sub-Saharan Africa and global averages. The maternal mortality rate in SSA stands at 454 per 100,000 live births, compared to the global average of 197 [20]. The under-five mortality rate is 72 per 1,000 live births, nearly double the global average of 37. The Universal Health Coverage (UHC) Service Coverage Index for SSA stands at 46, significantly below the target of 80. These health outcomes are strongly correlated with governance quality, with many SSA countries falling into the weak governance zone, below the 30th percentile, across multiple dimensions.

The persistent gap between SSA and global averages reflects decades of underinvestment in health system infrastructure and governance capacity. As illustrated in Fig. 2, governance quality varies significantly across SSA countries, with nations such as Rwanda and Botswana demonstrating that strong governance is achievable and directly correlates with better health system performance.

Structural Barriers to Digital Health Integration

Several interconnected structural barriers complicate efforts to integrate digital health into fragile governance environments. The successful deployment of digital health systems requires a workforce capable of operating them. However, SSA faces a projected shortage of 6.1 million health workers by 2030 [23]. Compounding this shortage is a widespread lack of digital literacy among existing healthcare professionals. Figure 3 presents the prevalence of these barriers as identified across 47 systematic reviews of digital health implementation in SSA.

Infrastructural and Connectivity Deficits

Despite the growth in mobile penetration, foundational infrastructure remains a critical bottleneck. An estimated 550 million people in Africa lack reliable access to electricity, and approximately 100,000 public health facilities operate without stable power or internet connectivity [10]. Only 22% of health facilities in SSA have reliable internet access, compared to the global average of 75%..

Fragmentation and Lack of Interoperability

The digital health landscape in SSA is highly fragmented. A study of digital health systems in Kenya revealed a multitude of disparate systems implemented by various donors and NGOs, most of which do not communicate with one another [13]. This lack of interoperability prevents the creation of unified patient records, duplicates data entry efforts for healthcare workers, and hinders national disease surveillance [14]. Figure 5 contextualizes this challenge within the broader trajectory of digital health adoption across SSA, demonstrating that rapid growth in mHealth users has not been matched by proportional investment in interoperability infrastructure.

Financing and Donor Dependency

Healthcare financing in SSA is heavily reliant on out-of-pocket payments and external donor funding. Consequently, digital health initiatives are frequently funded by international donors as short-term pilot projects. When donor funding cycles end, these projects collapse due to a lack of domestic budgetary integration and sustainable financing models [7]. The estimated digital health funding gap in Africa is approximately USD 4.1 billion for the period 2024 to 2030 [24], as illustrated in Fig. 6.

The Cybersecurity Imperative

The rapid digitization of health records and the deployment of connected medical devices have exponentially expanded the attack surface of African healthcare systems. The intersection of weak governance and poor cybersecurity infrastructure creates a highly permissive environment for cyber threat actors. The healthcare sector in Africa faces an average of 3,575 weekly attacks per organization, more than double the global average, as shown in Fig. 7 [15]. The threat landscape is dominated by phishing (38%), ransomware (27%), and data breaches targeting electronic medical records (18%; [17]).

The primary vulnerability is not merely technical, but regulatory. Many African nations lack comprehensive national cybersecurity strategies specific to the healthcare sector. Where data protection laws exist, they are often broad and lack the specific technical mandates required to secure health data [16]. Furthermore, the procurement of digital health solutions frequently prioritizes cost and speed over security, leading to the deployment of systems with inherent vulnerabilities and a dangerous reliance on third-party vendors with weak security postures [10,17].

Conceptual Framework: The Digital Health Governance Integration Model (DHGIM)

A central premise of this work is that digital health interventions in Sub-Saharan Africa fail not due to technological inadequacy, but because they are introduced into environments lacking the structural governance capacity to absorb, regulate, and sustain them. In response, we introduce the Digital Health Governance Integration Model (DHGIM), illustrated in Fig. 8. Unlike existing digital health frameworks that focus primarily on technological deployment or health system components independently, the DHGIM integrates governance, cybersecurity, and implementation processes into a unified systems model built on three interdependent pillars

Pillar 1: Structural Alignment

In weak governance systems, digital health is often driven by external donor priorities rather than national health strategies, leading to the "pilotitis" described throughout this paper. The DHGIM argues that the first step in integration is Structural Alignment, requiring a shift from project-based implementation to a National Enterprise Architecture (NEA) approach. An NEA acts as the blueprint for the health system, defining how different digital tools interact and share data. By mandating adherence to international interoperability standards such as HL7 FHIR, the NEA ensures that data flows seamlessly across the continuum of care, regardless of the vendor or donor funding the specific tool [21].

Pillar 2: Regulatory Fortification

The second pillar addresses the critical vulnerability of weak regulatory environments. Regulatory Fortification involves the establishment of a robust, enforceable legal and technical scaffolding that goes beyond mere compliance, requiring the proactive integration of cybersecurity into the procurement and design phases of digital health projects, a principle commonly referred to as security by design. Key components include national health data ownership policies establishing clear legal definitions of who owns patient data and the mechanisms for patient consent; mandatory security audits requiring all digital health vendors to undergo regular, independent cybersecurity assessments; and Health-CERTs, specialized Computer Emergency Response Teams dedicated to monitoring and responding to cyber threats within the national health infrastructure.

Pillar 3: Capacity Absorption

The final pillar is Capacity Absorption, which requires a dual focus. First, human capital development must move beyond basic software training to comprehensive digital literacy and cybersecurity hygiene, integrating health informatics into the core curricula of medical and nursing schools. Second, institutional resilience requires building the capacity of Ministries of Health to manage complex digital ecosystems, including establishing dedicated Digital Health Directorates with the authority to enforce the NEA, manage multi-stakeholder partnerships, and transition digital health financing from volatile donor grants to sustainable domestic budgets [24].

The DHGIM as a Feedback Loop

The DHGIM is not a linear progression but a continuous feedback loop. Structural Alignment provides the blueprint, Regulatory Fortification provides the secure environment, and Capacity Absorption provides the operational capability. As institutional capacity grows, it enables more sophisticated regulatory enforcement, which in turn allows for more complex structural alignment, including the integration of artificial intelligence and predictive analytics into the national health information architecture.

Discussion

The persistent failure of digital health initiatives to scale in Sub-Saharan Africa is not a technological shortcoming but a profound institutional failure. When complex digital systems are introduced into environments characterized by weak regulatory oversight and fragmented financing, they do not bypass these systemic weaknesses; they become entangled in them. The resulting “pilotitis” is a symptom of a broader political economy in which external donor priorities supersede national health sovereignty, leading to structural misalignment.

To translate the DHGIM into practice, we propose an Integrated Digital Health Policy Framework that operationalizes the model’s three governance pillars through the lens of the WHO’s six building blocks of health systems. It is important to distinguish between these two components. The DHGIM is a governance architecture: it establishes the structural conditions, Structural Alignment, Regulatory Fortification, and Capacity Absorption, that must be in place before any digital health intervention can be

sustained. The six-pillar framework is an implementation instrument: it translates those governance conditions into concrete policy actions mapped to each WHO building block. Figure 9 illustrates how each building block corresponds to a specific DHGIM pillar, demonstrating the theoretical coherence between governance design and implementation practice.

Six-Pillar Policy Framework

Pillar 1: Leadership and governance

Effective digital health integration requires strong leadership and institutional capacity. Governments must establish dedicated digital health agencies or directorates within Ministries of Health, endowed with the authority and budget to coordinate all digital health activities, enforce compliance with national strategies, conduct regular governance audits, and manage multi-stakeholder partnerships [7].

Pillar 2: Health Information System

Digital health cannot function without a reliable physical foundation. Policies must incentivize public-private partnerships to expand broadband connectivity and reliable electricity to rural and underserved health facilities, including zero-rating access to essential health applications and investing in solar-powered solutions for off-grid clinics [10].

Pillar 3: Medical Product and Technology

Cybersecurity must be integrated into the foundational architecture of all digital health systems. Governments should adopt the NIST Cybersecurity Framework 2.0 as the baseline standard for digital health procurement, enact comprehensive health data protection regulations, mandate regular security audits for all digital health vendors, and establish national Health Computer Emergency Response Teams to monitor and respond to cyber threats [17,18].

Pillar 4: Workforce Capacity and Digital Literacy

The health workforce must be equipped to utilize digital tools effectively. This requires integrating digital health informatics into the curricula of medical and nursing schools and establishing continuous professional development programs to train existing staff in both software use and basic cybersecurity hygiene and data management [10].

Pillar 5: Financing and Sustainability

To reduce donor dependency, governments must develop sustainable domestic financing models for digital health. This involves integrating digital health budgets into national health financing strategies, exploring innovative funding mechanisms such as remittance-based insurance or digital health taxes, and transitioning from capital expenditure models to operational expenditure models through cloud computing and software-as-a-service [24].

Pillar 6: Service Delivery

To eliminate data silos, governments must mandate adherence to international interoperability standards such as HL7 FHIR and ICD-10. The establishment of a National Health Information Exchange architecture is critical to ensure that disparate systems can communicate, enabling continuity of care and comprehensive public health surveillance [21].

Implementation Roadmap

The transition to a mature digital health ecosystem in a weak governance environment cannot occur overnight. Table 2 presents a phased implementation roadmap to guide policymakers through this transformation. Each phase builds on the preceding one, expanding governance capacity before scaling technical infrastructure.

Table 2

Phased Implementation Roadmap for the Digital Health Governance Integration Model (DHGIM). NEA = National Enterprise Architecture; CERT = Computer Emergency Response Team; EHR = Electronic Health Record; HMIS = Health Management Information System; TAPIC = Transparency, Accountability, Participation, Integrity, Capacity.

Phase	Timeframe	Focus	Key Actions
Phase 1: Foundation and Assessment	Years 1–2	Establish legal, regulatory, and audit infrastructure	Enact or strengthen health data protection legislation; conduct governance and infrastructure audits across health facilities; develop a costed National Digital Health Strategy aligned to the NEA; establish a National Health CERT; map existing pilot projects for interoperability assessment.
Phase 2: Infrastructure and Capacity Building	Years 2–4	Build foundational digital infrastructure and workforce capacity	Invest in connectivity and power infrastructure for health facilities; implement large-scale digital health workforce training programs; deploy secure, interoperable pilot projects using HL7 FHIR standards; establish vendor security certification requirements in public procurement.
Phase 3: Scale-Up and Integration	Years 4–6	Roll out national systems and enforce interoperability standards	Deploy national EHR and telemedicine networks; enforce interoperability standards across all public health facilities; integrate digital health data into the national HMIS; conduct mid-term DHGIM governance audit against TAPIC dimensions; publish national data sovereignty frameworks.
Phase 4: Sustainability and Innovation	Year 6+	Transition to domestic financing and advanced analytics	Transition from donor-dependent to domestically financed digital health budgets; integrate AI and predictive analytics into national health modeling, with explicit algorithmic bias governance; conduct full DHGIM ecosystem evaluation; publish national digital health lessons for regional peer learning.

Suggestions for Future Research

While this study provides a comprehensive framework for integrating digital health into weak governance systems, several avenues for future research remain. First, empirical studies are needed to test the efficacy of the DHGIM in specific country contexts. Longitudinal research tracking the implementation of National Enterprise Architectures could provide valuable insights into the practical challenges of structural alignment. Second, as artificial intelligence and machine learning become more prevalent in healthcare, research must explore how these advanced technologies can be safely deployed in environments with nascent regulatory frameworks, particularly investigating ethical implications and algorithmic biases in diverse African populations. Finally, further investigation into sustainable domestic

financing models for digital health is essential to reduce donor dependency and ensure long-term system resilience.

Conclusions

The integration of digital health technologies holds immense potential to strengthen health systems and accelerate progress toward Universal Health Coverage in Sub-Saharan Africa. However, this potential is currently constrained by weak governance, fragmented implementation, and escalating cybersecurity threats. The failure of digital health initiatives in the region is rarely a failure of technology; it is a failure of policy, planning, and institutional capacity.

The DHGIM proposed in this paper offers a governance-centric alternative to the prevailing technology-first approach. By positioning structural alignment, regulatory fortification, and capacity absorption as the foundational pillars of digital health integration, the model provides a practical roadmap for policymakers navigating the complex intersection of digital transformation and fragile governance. The framework is not prescriptive; it is designed to be adapted to the specific political, economic, and institutional contexts of individual countries.

Ultimately, this research suggests that for digital health to succeed in fragile environments, it must be underpinned by a robust, integrated policy framework. By prioritizing governance, interoperability, cybersecurity, and sustainable financing, policymakers can transform digital health from a series of disjointed pilot projects into a resilient national infrastructure. As Sub-Saharan Africa navigates its digital transformation, the focus must shift from merely acquiring technology to building the institutional and human capacity required to govern it effectively. Only through such a comprehensive approach can digital health fulfill its promise of delivering equitable, secure, and high-quality healthcare to all.

Declarations

Ethics Approval and Consent to Participate

This research constitutes a policy analysis and systematic review of publicly available, anonymized secondary data and literature. As it does not involve human subjects, primary clinical data, or animal experiments, formal ethical approval and consent to participate were not required in accordance with standard institutional review board guidelines.

Availability of Data and Materials

The datasets analyzed during the current study are publicly available from the WHO Global Health Observatory (<https://www.who.int/data/gho>), the World Bank DataBank (<https://databank.worldbank.org/>), and UNICEF (<https://data.unicef.org/>).

Competing Interests

The authors declare that they have no competing interests.

Funding

The authors declare that no specific funding was received for this study.

Authors' Contributions

A. C.-P. conceptualized the study, conducted the policy analysis, and drafted the sections on governance and health system strengthening. E. N. B. F. conducted the cybersecurity analysis, developed the data visualizations, and drafted the sections on data governance and the policy framework. Both authors read and approved the final manuscript.

Author Note

Alplato Chukpue-Padmore, Center for Integrated Solutions, Monrovia, Liberia; Emmanuel N. B. Flomo, Cybersecurity Analyst. Correspondence concerning this article should be addressed to Alplato Chukpue-Padmore. Email: chukpuepadmore2019@gmail.com

References

1. UNICEF. Child mortality data: Under-five mortality rate. UNICEF; 2024. Available from: <https://data.unicef.org/topic/child-survival/under-five-mortality/>
2. World Health Organization. Trends in maternal mortality 2000 to 2023. Geneva: WHO; 2023. Available from: <https://www.who.int/publications/i/item/9789240068759>
3. Awosiku OV, Okonkwo UP, Eze CN, Adeyemi OA. Role of digital health technologies in improving health financing and universal health coverage in Sub-Saharan Africa. *Front Digit Health*. 2025;7:Article 1391500. <https://doi.org/10.3389/fdgth.2025.1391500>
4. Grand View Research. Africa digital health market size, share & trends analysis report, 2024-2030. San Francisco: Grand View Research; 2024. Available from: <https://www.grandviewresearch.com/industry-analysis/africa-digital-health-market-report>
5. Dugani SB, Afari H, Hirschhorn LR, Ratcliffe H, Veillard J, Martin G, et al. Digitalization of health care in low- and middle-income countries. *Bull World Health Organ*. 2024. Available from: <https://cdn.who.int/media/docs/default-source/bulletin/online-first/blt.24.291643.pdf>
6. Sylla B, Diallo A, Kourouma M, Balde A. African digital health strategic plans analysis: Key weaknesses in contextualization, intervention focus, and technological foresight. *NPJ Digit Med*. 2025;8:748. Available from: <https://pmc.ncbi.nlm.nih.gov/articles/PMC12680716/>
7. Mengiste SA, Kaasboll J, Haslie A, Soriyan A. eHealth policy framework in low and lower middle-income countries: A PRISMA systematic review and analysis. *BMC Health Serv Res*. 2023;23:328. Available from: <https://pmc.ncbi.nlm.nih.gov/articles/PMC10067308/>

8. Jiwa A. Africa's digital health revolution: The digital fit-viability challenge. *NPJ Cardioasc Health*. 2025. Available from: <https://pmc.ncbi.nlm.nih.gov/articles/PMC12912428/>
9. GSMA. The mobile economy Africa 2024. London: GSMA; 2024. Available from: <https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/africa/>
10. Segun-Omosehin OA, Okonkwo CA, Adeyemo AO, Eze CN. Evaluating the digital health technology landscape in sub-Saharan Africa and its implications for cardiovascular health. *NPJ Cardioasc Health*. 2025. Available from: <https://www.nature.com/articles/s44325-025-00055-9>
11. World Bank. Worldwide governance indicators. Washington, DC: World Bank DataBank; 2023. Available from: <https://databank.worldbank.org/source/worldwide-governance-indicators>
12. Kouadio M. Effects of governance quality on health outcomes in West African countries. *Discov Public Health*. 2025;22:645. <https://link.springer.com/article/10.1186/s12982-025-01014-6>
13. Ireri S, Wambua P, Kimani S, Mwangi J. An exploration of the successful scale-up of the electronic community health information system in Kenya. *Oxford Open Digit Health*. 2025. <https://academic.oup.com/oodh/article/doi/10.1093/oodh/oqaf020/8253486>
14. Muinga N, Magare S, Monda J, English M, Fraser H, Powell J, et al. Digital health systems in Kenyan public hospitals: A mixed-methods survey. *BMC Med Inform Decis Mak*. 2020;20:2. Available from: <https://pmc.ncbi.nlm.nih.gov/articles/PMC6945428/>
15. Microsoft. Healthcare under attack: Why cybersecurity is now critical care. Microsoft Threat Intelligence; 2026. Available from: <https://news.microsoft.com/source/emea/features/healthcare-under-attack-why-cybersecurity-is-now-critical-care/>
16. McKay AGN, Mwangi B. The regulation of health data sharing in Africa: A comparative study. *J Law Biosci*. 2024;11(1):lsad035. <https://academic.oup.com/jlb/article/11/1/lsad035/757765>
17. Digital Health Africa. When innovation outpaces protection: Closing the cybersecurity gap in Africa's healthcare. *Digital Health Africa*; 2025. Available from: <https://digitalhealth-africa.org/when-innovation-outpaces-protection-closing-the-cybersecurity-gap-in-africas-healthcare/>
18. National Institute of Standards and Technology. Cybersecurity framework 2.0. Gaithersburg: U.S. Department of Commerce; 2024. Available from: <https://www.nist.gov/cyberframework>
19. Hsieh HF, Shannon SE. Three approaches to qualitative content analysis. *Qual Health Res*. 2005;15(9):1277-88. <https://doi.org/10.1177/1049732305276687>
20. World Health Organization, United Nations Children's Fund, United Nations Population Fund, World Bank Group, United Nations Department of Economic and Social Affairs. Trends in maternal mortality 2000 to 2023: Estimates by WHO, UNICEF, UNFPA, World Bank Group and UNDESA/Population Division. Geneva: WHO; 2024. Available from: <https://www.who.int/publications/i/item/9789240108462>
21. Smart Africa Alliance. Digital health blueprint. Kigali: Smart Africa; 2025. Available from: <https://smartafrica.org/wp-content/uploads/2025/11/Digital-Health-Blueprint-English-2.pdf>
22. Greer SL, Wismar M, Figueras J, editors. Strengthening health system governance: Better policies, stronger performance. Maidenhead: Open University Press / WHO Regional Office for Europe; 2019.

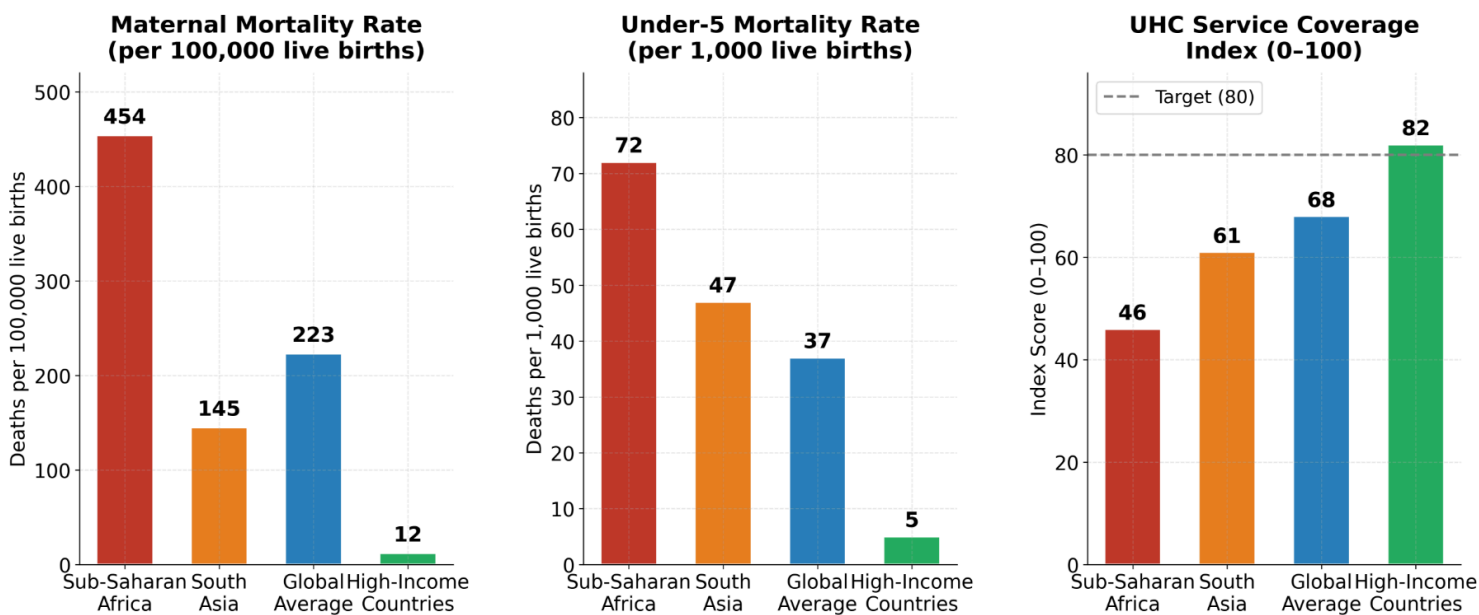
Available from: <https://eurohealthobservatory.who.int/publications/m/strengthening-health-system-governance-better-policies-stronger-performance>

23. Asamani JA, Christmals CD, Reitsma GM. State of the health workforce in the WHO African Region: Decade review of progress and opportunities for policy reforms and investments. *BMJ Glob Health*. 2024;9(1):e015952. <https://doi.org/10.1136/bmjgh-2024-015952>

24. Transform Health Coalition. Ensuring more and better funding for digital health transformation. Washington, DC: Transform Health Coalition; 2023. Available from: <https://transformhealthcoalition.org/>

Figures

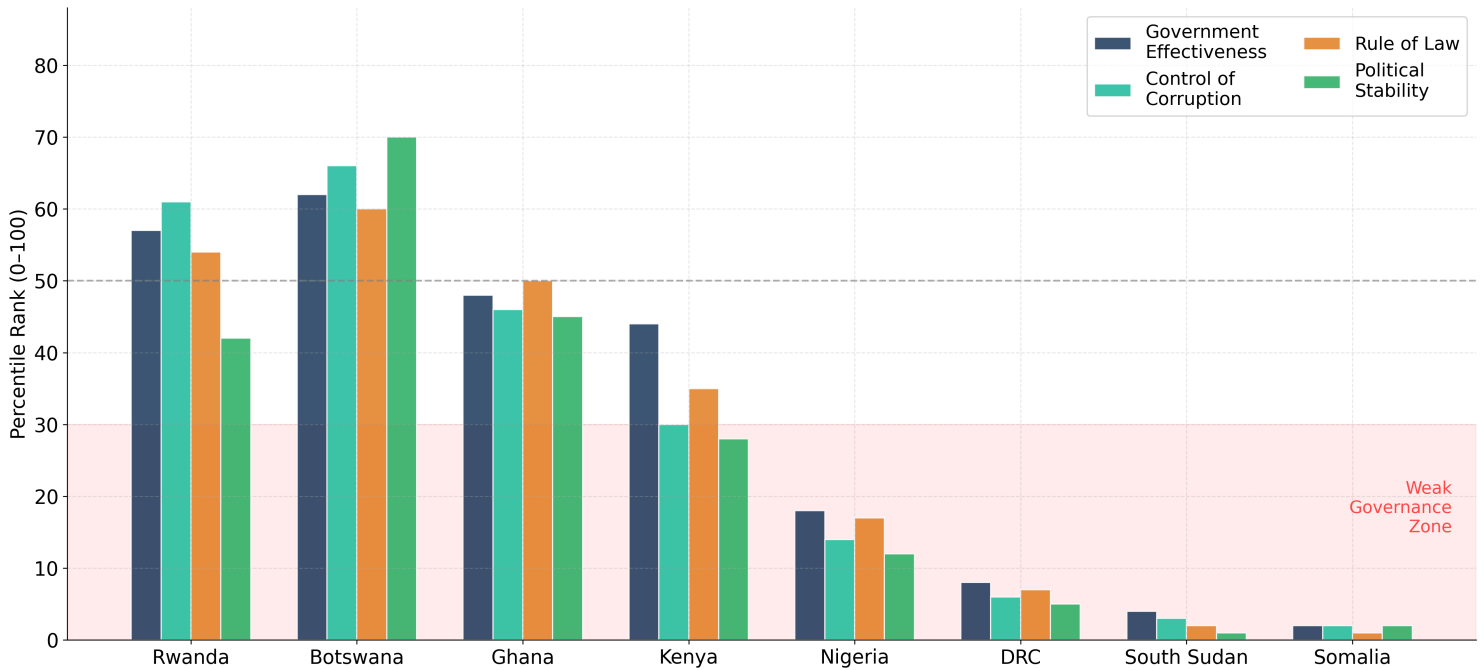
Figure 1. Key Health Burden Indicators: Sub-Saharan Africa vs. Global Averages (2023)



Sources: WHO Maternal Mortality Report (2023); UNICEF Child Mortality Data (2024); World Bank UHC Service Coverage Index (2023).

Figure 1

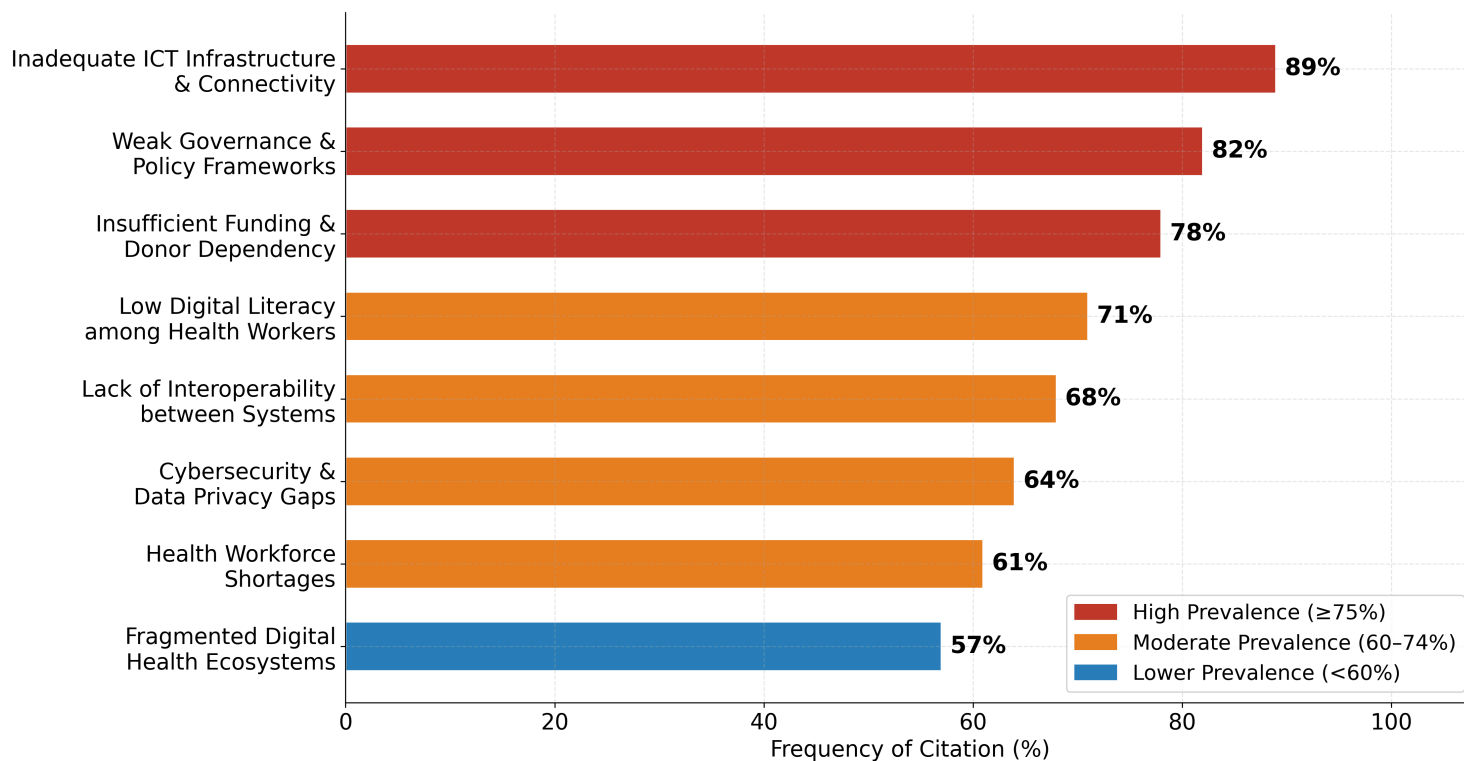
Key health burden indicators: Sub-Saharan Africa vs. global averages (2023). Sources: WHO Maternal Mortality Report [2]; UNICEF Child Mortality Data [1]; World Bank UHC Service Coverage Index [11].



Source: World Bank Worldwide Governance Indicators (2023). Note: Percentile ranks are approximate estimates based on published WGI data.

Figure 2

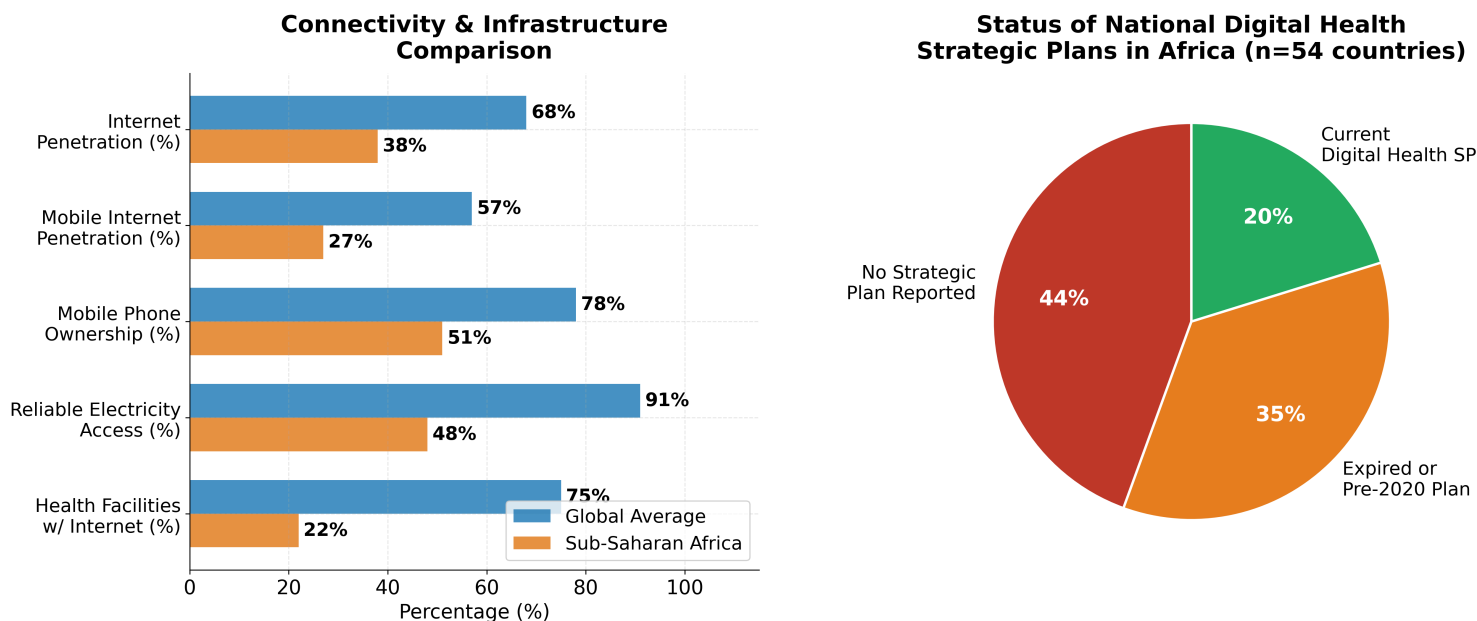
World Bank governance indicators for selected Sub-Saharan African countries (2023). Source: World Bank Worldwide Governance Indicators [11]. Note: Percentile ranks are approximate estimates based on published WGI data.



Sources: Synthesized from Segun-Omosehin et al. (2025); Mengiste et al. (2023); Sylla et al. (2025).

Figure 3

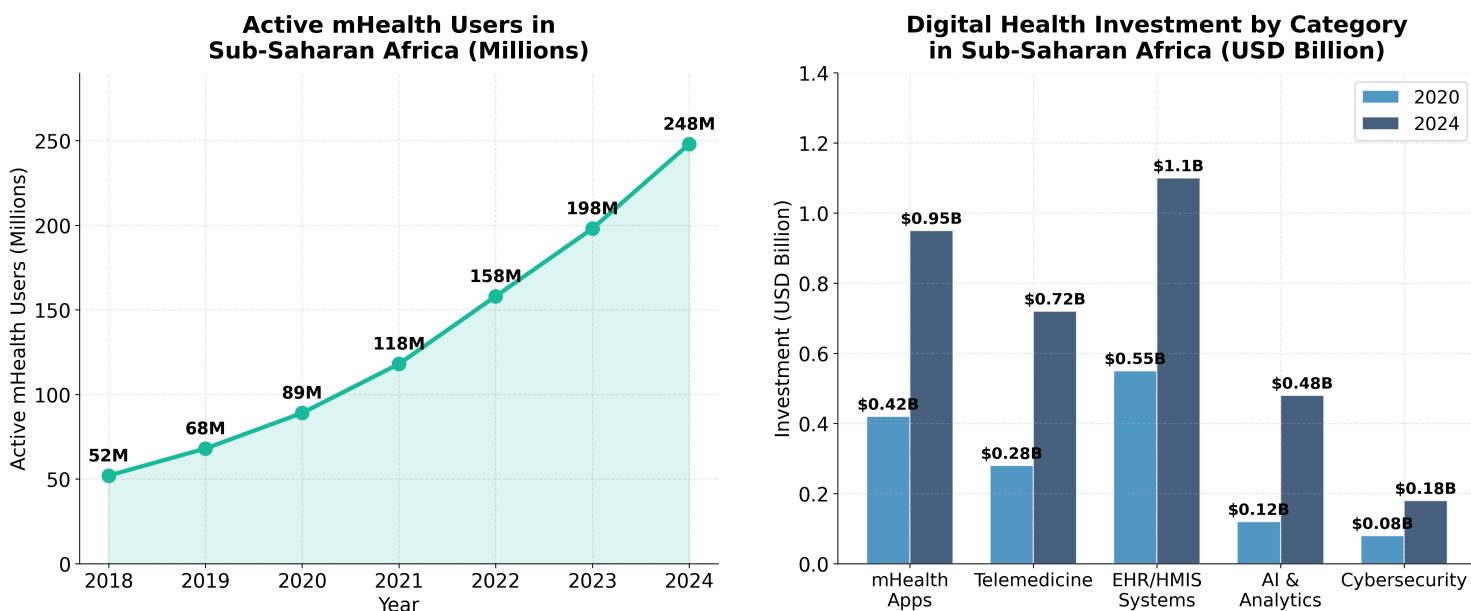
Prevalence of barriers to digital health implementation in Sub-Saharan Africa (frequency of citation in systematic reviews, n = 47 studies). Sources: Segun-Omosehin et al. [10]; Mengiste et al. [7]; Sylla et al. (2025).



Sources: GSMA Mobile Economy Sub-Saharan Africa (2024); World Bank Data (2024); Sylla et al., NPJ Digital Medicine (2025); USAID Digital Health Estimates.

Figure 4

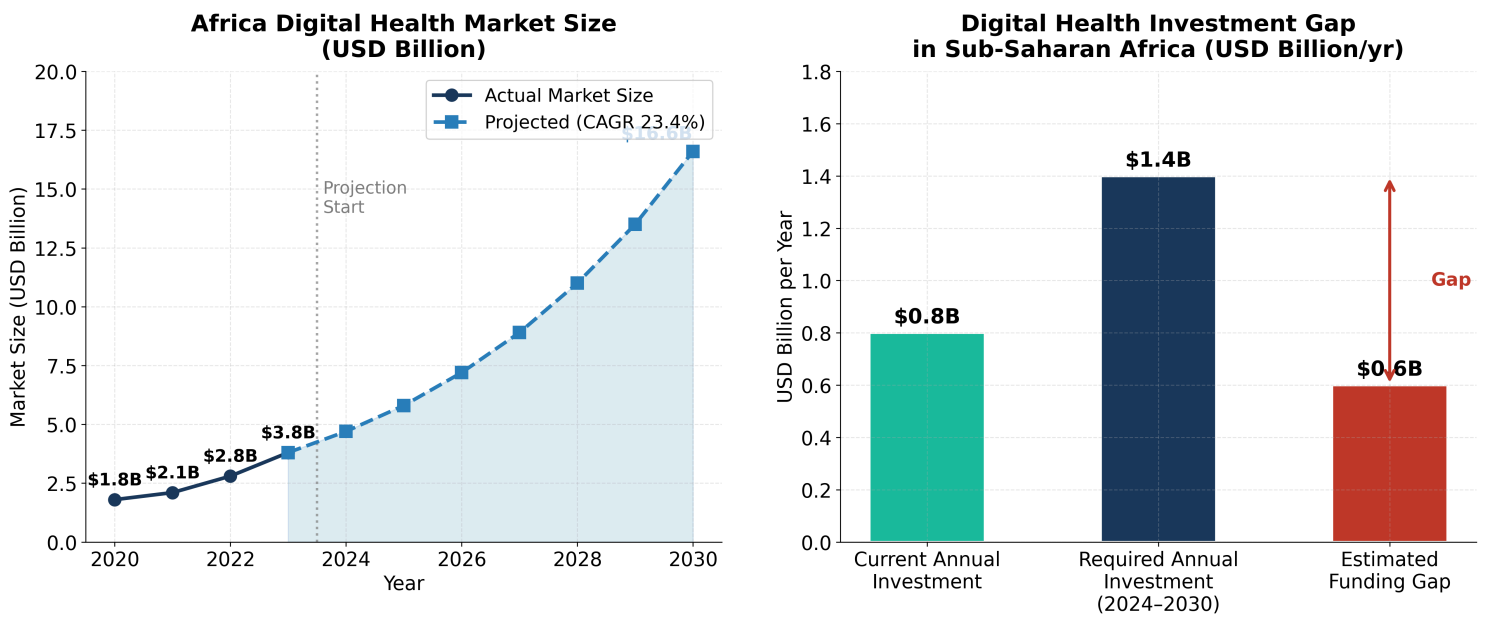
Digital health infrastructure gaps in Sub-Saharan Africa (2023 to 2024). Sources: GSMA Mobile Economy Sub-Saharan Africa [9]; World Bank Data [11]; Sylla et al. [6]; USAID Digital Health Estimates



Sources: GSMA Mobile Economy Sub-Saharan Africa (2024); Grand View Research (2024); WHO Global Health Observatory (2024).

Figure 5

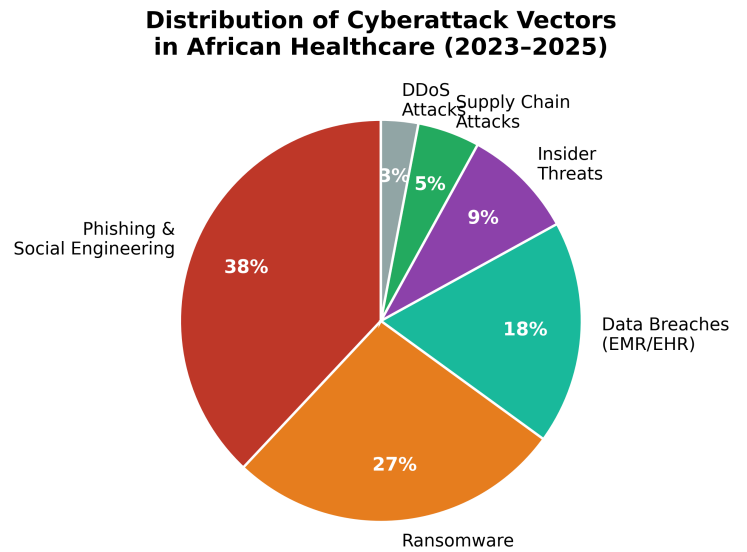
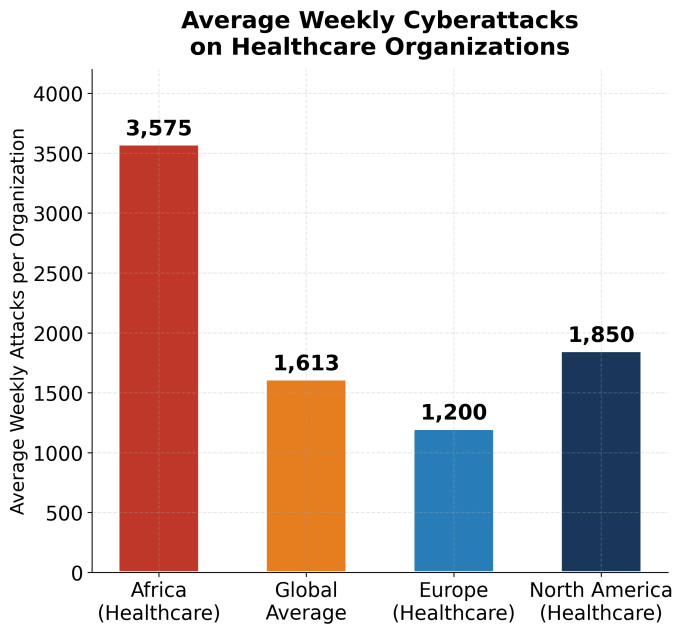
Digital health adoption trends in Sub-Saharan Africa (2018 to 2024). Sources: GSMA [9]; Grand View Research [4]; WHO Global Health Observatory (2024).



Sources: Grand View Research (2024); Transform Health Coalition (2023). Investment gap estimated at ~USD 4.1B over 2024-2030.

Figure 6

Africa digital health market growth and investment gap (2020 to 2030). Sources: Grand View Research [4]; Transform Health Coalition [24].



Sources: Microsoft Threat Intelligence Report (2026); Digital Health Africa (2025).

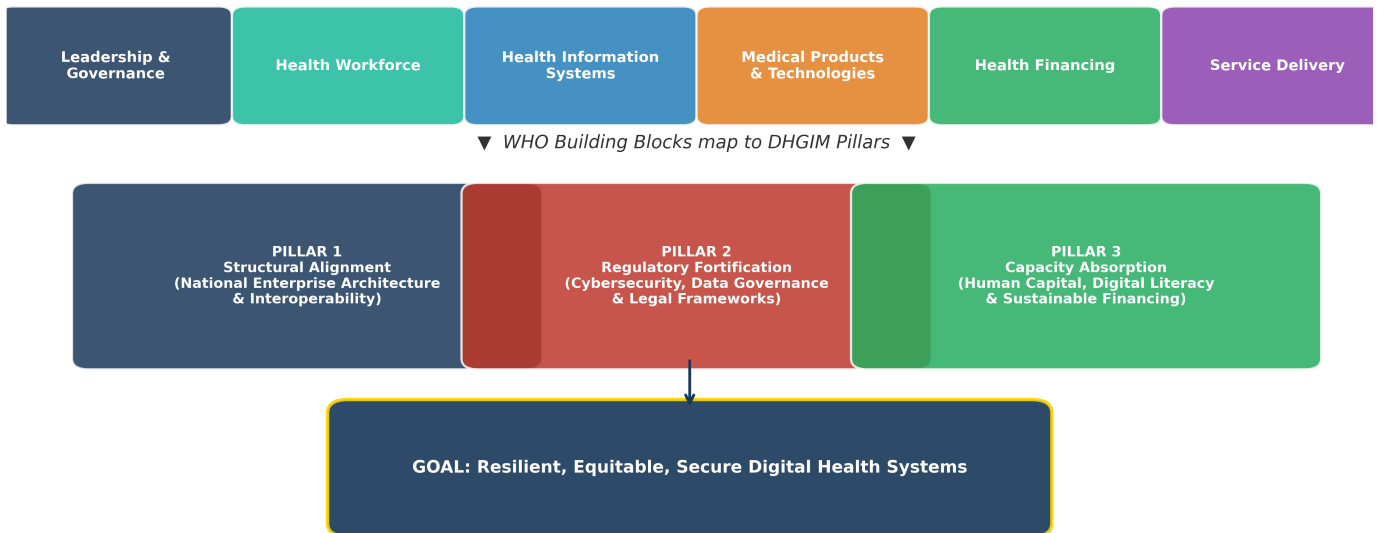
Figure 7

Cybersecurity threat landscape in African healthcare systems (2023 to 2025). Sources: Microsoft Threat Intelligence Report [15]; Digital Health Africa [17].

Image not available with this version

Figure 8

Legend not included with this version.



Note: Adapted from WHO (2007). Everybody's Business: Strengthening Health Systems. DHGIM pillar alignment proposed by the authors.

Figure 9

WHO six building blocks of health systems and DHGIM pillar alignment. Note: Adapted from WHO (2007). DHGIM pillar alignment proposed by the authors.