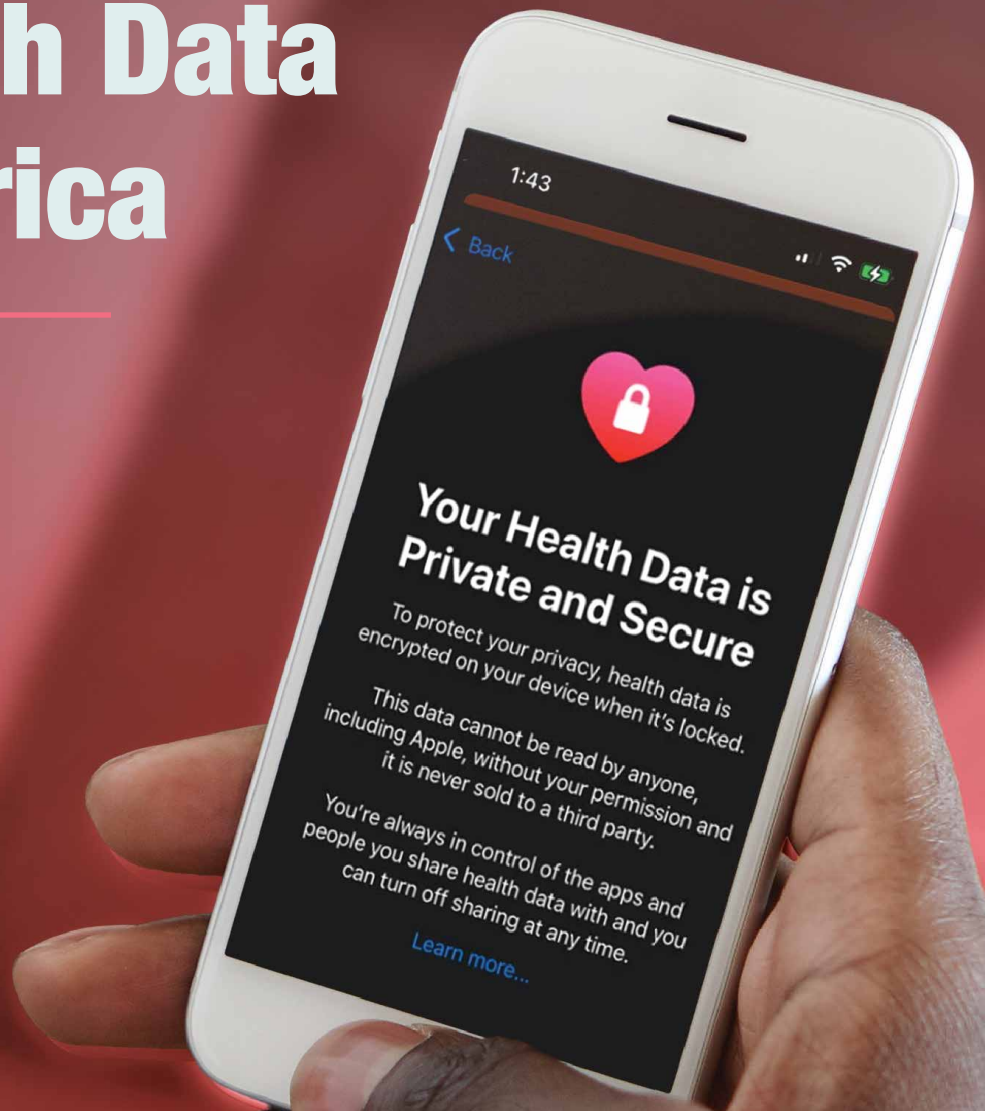
Towards Regulation of App-Based Health Data in Africa

June, **2026**



CIPESA

1. Introduction

Digital health technologies are reshaping healthcare delivery across Africa. App-based systems now connect patients, clinicians, pharmacies, laboratories, and public health agencies, creating new opportunities to improve access, efficiency, and coordination of care. At the same time, they generate large volumes of highly sensitive health data, much of it moving across platforms, providers, and, in some cases, national borders.

This rapid expansion has outpaced the capacity of existing governance frameworks. In many African countries, health data is still regulated through fragmented legal and institutional systems that were not designed for platform-based services, cross-border data flows, or artificial intelligence (AI)-enabled decision-making. As a result, consent practices are often weak, accountability is unclear, and users have limited control over how their data is collected, shared, stored, or reused.

This brief examines why app-based health data should be regulated in Africa and outlines the principles that should guide that regulation.

2. The Case for Regulating App-Based Health Data

Across the continent, digital health applications now span multiple functions within health systems. Clinical management systems and electronic medical records (EMR) platforms are being used in countries including Cameroon, Kenya, Ghana, Nigeria,[1] Rwanda,[2] South Africa, and Uganda to digitise patient data and support clinical workflows, including in areas such as HIV care, maternal and child health, and general service delivery.[3]

Alongside these systems, AI-enabled and specialist care platforms are expanding diagnostic and treatment capacity. Examples include Rology for AI-assisted teleradiology and diagnostics in Egypt, Ethiopia and Tanzania; Dawa Health in Zambia and Zimbabwe, which assists maternal health care; DeepEcho in South Africa, which is focused on AI-enabled cardiac care; and the Vula Mobile in South Africa that connects primary health workers in rural areas with specialists. In Nigeria, Ubenwa, an AI-powered platform, monitors baby cries to analyse needs and health.[4]

Digital innovation is also transforming pharmaceutical logistics and supply chains. Platforms such as mPharma in Ghana support medicine inventory management, while LifeBank in Nigeria and Kenya facilitates rapid delivery of blood, oxygen, and essential medical supplies. In Egypt, platforms such as Chefaa provide AI-enabled medicine ordering and delivery services, improving access to essential drugs.

Patient-facing applications are also expanding, particularly in chronic care, maternal health, and home-based services. Platforms such as MomConnect in South Africa and MyQura in Nigeria support patient engagement and follow-up care, while services such as Labtracka in Nigeria facilitate laboratory booking, sample collection, and results delivery.

While these innovations are improving access to services and efficiency, they also introduce significant governance risks. Health data is among the most sensitive categories of personal data, capable of revealing medical history, reproductive health, mental health status, and genetic information. In app-based systems, this data is often processed by multiple actors, including developers, health providers, cloud infrastructure providers, and third-party analytics firms, many of which are not visible to users.

In practice, consent is often weak or poorly understood, data sharing arrangements are opaque, and users have limited visibility or control over downstream use of their information. This creates risks not only to privacy but also to trust in digital health systems.

These risks are compounded by fragmented legal and institutional frameworks. Although many countries have enacted data protection laws and digital health policies, enforcement remains uneven and coordination between health ministries, data protection authorities, and digital regulators is often weak. This creates a persistent governance gap between the rapid expansion of app-based health systems and the capacity of institutions to regulate them effectively.

At the continental level, emerging frameworks such as the African Union (AU) Continental Health Data Governance Framework and global guidance such as the World Health Organisation (WHO) Digital Health Strategy set important normative directions for secure, rights-respecting health data governance.[5] However, translating these commitments into enforceable national systems remains limited, particularly in relation to interoperability, cross-border data flows, and platform accountability.

1 Akwaowo, Christie Divine, Humphrey Muki Sabi, Nnette Ekpenyong, Chimaobi M. Isiguzo, Nene Francis Andem, Omosivie Maduka, Emem Dan, Edidiong Umoh, Victory Ekpin, and Faith-Michael Uzoka. "Adoption of electronic medical records in developing countries—A multi-state study of the Nigerian healthcare system." Frontiers in Digital Health 4 (2022): 1017231.

2 Rwanda, Data Protection and Privacy Law Law No 058/2021 of 13/10/2021, https://www.risa.gov.rw/data-protection-and-privacy-law

3 Kavuma, Michael. "The usability of electronic medical record systems implemented in sub-Saharan Africa: a literature review of the evidence." JMIR human factors 6, no. 1 (2019): e9317.

4 Ephraim, Richard Kobina Dadzie, Gabriel Pezahso Kotam, Evans Duah, Frank Naku Ghartey, Evans Mantiri Mathebula, and Tivani Phosa Mashamba-Thompson. "Application of medical artificial intelligence technology in sub-Saharan Africa: prospects for medical laboratories." Smart Health 33 (2024): 100505.

5 Africa CDC, 'Africa CDC statement on the outcomes of the 39th ordinary session of the African Union Assembly' (23 February 2026) https://africacdc.org/news-item/africa-cdc-statement-on-the-outcomes-of-the-39th-ordinary-session-of-the-african-union-assembly/

3. The Existing National and Continental Regulatory Frameworks

At the continental level, several instruments provide an important foundation. The African Union Convention on Cyber Security and Personal Data Protection[6] establishes baseline standards for data protection and cybersecurity across member states, although its impact remains limited by slow ratification and uneven implementation. The AU Data Policy Framework (2022) advances a more integrated governance approach, calling for harmonised data systems, a continental Digital Single Market, and a balanced approach to data sovereignty and cross-border data flows. The AU Continental AI Strategy (2024) extends this architecture to artificial intelligence, including its use in public service delivery and health systems, and reinforces the need for accountable and rights-centred AI governance.

Most significantly for digital health, the Africa Centre for Disease Control (CDC) Continental Health Data Governance Framework sets out principles on active consent, interoperability, and secure health data governance, including alignment with the Fast Healthcare Interoperability Resources (FHIR) standard. Together, these instruments outline an emerging continental governance architecture for digital health. However, implementation remains limited, and most member states have yet to domesticate these frameworks into enforceable regulatory systems or operational practice.

At least 44 African countries have enacted data protection laws,[7] many of which classify health data as sensitive and subject it to enhanced safeguards. Many countries have established Data protection Authorities (DPAs) that increasingly exercise jurisdiction over digital platforms, including health applications. Some countries are also introducing data localisation requirements, with Nigeria, Kenya, and South Africa among those taking steps to require that sensitive health data is stored within national or regional infrastructure.[8]

Health-specific legislation is emerging but remains fragmented in scope and ambition. Kenya's Digital Health Act 2023[9] establishes a regulatory framework for digital health information systems and platform governance. South Africa's National Health Insurance Act, 2023 strengthens protections for patient data and electronic health records within the public health system.[10] Nigeria's National Health Act,[11] alongside data protection laws in Ghana [12] and Rwanda, provide a broader legal basis for health data governance. Egypt has enacted a comprehensive data protection legislation and is advancing a national digital health strategy with implications for app-based health services. [13]

Despite these developments, important governance gaps remain. The first is the absence of health-specific AI governance. Existing frameworks were designed for conventional digital environments and do not adequately address the risks introduced by AI-enabled diagnostic tools, predictive systems, and automated clinical decision support. Algorithmic accountability, bias detection, and the use of African population data in model training and validation remain insufficiently regulated, despite the growing deployment of these systems in health contexts.

The second is institutional fragmentation. Responsibility for governing app-based health systems is dispersed across health ministries, data protection authorities, communications regulators, and in some cases, pharmaceutical and medical device regulators. Weak coordination between these institutions creates regulatory gaps, overlapping mandates, and limited pathways for user accountability and redress.

6 African Union Convention on Cyber Security and Personal Data Protection, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

7 Digital Policy Alert, "The Year of the Teeth: Data Protection in Africa Roundup," 11 January 2026, https://digitalpolicyalert.org/blog/data-protection-in-africa-roundup

8 Kapsule Research Team, "Health Data Privacy in Africa: Regulatory Guide for Research and Development," 28 February 2026, https://kapsuletech.com/blog/health-data-privacy-africa/

9 The Digital Health Act No.15 of 2023, https://nhts.dha.go.ke/api/file-download/?filename=Digital%20Health%20Act%2015%20of%202023.pdf

10 National Health Insurance Act 2023, https://www.gov.za/sites/default/files/gcis_document/202405/50664nathealthinsuranceact202023.pdf

11 Nigeria's National Health Act, 2014, https://scorecard.prb.org/wp-content/uploads/2019/06/Nigeria-National-Health-Act-2014.pdf

12 Ghana's Data Protection Act, 2012 (Act 843), https://nca.org.gh/wp-content/uploads/2020/09/Data-Protection-Act-2012.pdf

13 Law No. 151 of 2020 Promulgating the Personal Data Protection Law, https://www.acc.com/sites/default/files/program-materials/upload/Data%20Protection%20Law%20-%20Egypt%20-%20EN%20-%20MBH.PDF

The third is the unresolved distinction between wellness and clinical data. Most frameworks treat health data as a single category, despite the fact that app-based systems increasingly blur the boundaries between wellness tracking, behavioural monitoring, and clinical care. Without clearer classification frameworks, regulators risk applying inconsistent safeguards to data that may shift between wellness and clinical use within the same platform, weakening both user protection and enforcement capacity.

These gaps reflect the speed at which digital health innovation has advanced relative to slower cycles of legislative reform and institutional adaptation. The principles that follow provide a framework for addressing them in ways that are practical, rights-respecting, and grounded in the realities of African health systems.

4. Principles for Regulating App-Based Health Data

The effective governance of app-based health systems should be grounded in principles that balance innovation, public health needs, and rights protection. These principles can guide the design of legislation, regulation, and oversight mechanisms across Africa, ensuring that rapidly expanding app-based health data flows remain accountable, interoperable, and equitable. They should also align with emerging continental and global frameworks, including the Africa CDC Health Data Governance Framework, the AU Data Policy Framework, and the WHO Digital Health Strategy, all of which emphasise harmonised, rights-respecting, and secure data governance systems.

4.1 Data Sovereignty

Data sovereignty means that African states and the communities from which health data is generated should retain meaningful control over how that data is collected, stored, used, and shared. In the health sector, this is not only a matter of national interest but also of protecting sensitive personal information from extractive, opaque, or harmful practices. Health data should therefore be governed in ways that reflect African public health priorities, democratic oversight, and clearly defined accountability mechanisms, while ensuring that commercial interests do not override the rights and interests of patients and communities.

This does not mean closing off data flows or rejecting collaboration. It means establishing clear and enforceable rules on where data may be stored, who may access it, how it may be used, and conditions under which it may be transferred or repurposed. Regulatory frameworks should guard against unauthorised commercial exploitation of health data and ensure that African institutions retain the authority to audit, review, and restrict its use where necessary. A strong data sovereignty framework helps build trust in digital health systems while safeguarding public interest and institutional accountability.

4.2 Cross-Border Data Flows

Cross-border health data flows are essential for public health, research, and coordinated responses to disease outbreaks. However, these flows must be governed in ways that are secure, transparent, and consistent with human rights standards. Regulation should therefore enable data movement across borders where adequate and comparable safeguards exist, while preventing arbitrary restrictions that undermine cooperation and delay collective responses to shared health challenges.

What is required is a trusted regional approach rather than blanket data localisation or unrestricted data transfer. African countries should develop common standards for cross-border health data governance, supported by reciprocal recognition arrangements among DPAs and other competent institutions. These arrangements can enable disease surveillance, health research, and emergency response while ensuring accountability for breaches, misuse, and unauthorised disclosure. In this way, regional data sharing can remain both functional and rights-respecting.

Secure and regulated cross-border data flows can create what are increasingly referred to as "regional data flow trusted zones", in which health data moves between jurisdictions under harmonised safeguards, clear accountability mechanisms, and strong oversight, rather than through total bans on transboundary transfers.

4.3 Consent, Purpose Limitation, and Data Minimisation

Consent remains a key safeguard in app-based health systems, but in practice it is often weak, unclear, or embedded in complex and inaccessible terms. Users should be able to clearly understand how their health data is collected, shared, and reused. Consent should therefore be meaningful, specific, and accessible, enabling individuals to make informed decisions about participation in digital health systems.

However, consent alone is not sufficient. Health apps and related platforms should collect only the data necessary for clearly defined clinical, public health, or service delivery purposes. Secondary uses such as commercial profiling, behavioural targeting, or unrelated research should be tightly regulated and subject to explicit safeguards. Regulatory frameworks should require clear consent mechanisms, including layered or step-by-step consent where appropriate, alongside transparent records of data sharing across the data lifecycle.

4.4 Interoperability and Standardisation

Interoperability is essential for continuity of care, portability of health records, and efficient service delivery. Without common standards, app-based health systems risk creating fragmented data silos, locking users into proprietary platforms, and undermining coordinated healthcare delivery. In such environments, even beneficial innovations can become barriers to access and system integration.

Regulatory frameworks should therefore require compliance with recognised interoperability standards and, where health applications interface with public systems, certification against those standards. This should apply across electronic medical records, health information exchanges, and approved digital health platforms. [14] Interoperability should be treated as a public interest requirement that supports portability, reduces vendor lock-in,[15] and enables health systems to integrate new tools without compromising data integrity or patient rights.

14 *See for instance, Ministry of Health-Uganda, "The Uganda Health Data Access, Sharing and Use Guidelines, 2025, pp.8-10.*

15 *World Health Organization, "Global Strategy on Digital Health 2020-2027, 2025," p.22*

4.5 AI Governance

AI-enabled health tools are increasingly used for diagnosis, triage, risk prediction, and clinical decision support. While these systems can improve efficiency and expand access to care, they also introduce governance risks when trained on incomplete, unrepresentative, or poorly documented datasets. In African contexts, a key concern is that externally developed systems may not perform adequately for local populations, resulting in inaccurate outputs, uneven treatment outcomes, or hidden forms of discrimination.[16]

Regulatory frameworks should require algorithmic impact assessments, independent audits, and ongoing monitoring of AI-enabled health tools before and after deployment. Developers and service providers should demonstrate how systems were trained, what data was used, how performance was validated, and what safeguards exist to detect and correct bias or error.

Where AI is used in high-impact settings such as maternal health, infectious disease control, or clinical decision support, regulatory oversight should be proportionately stronger. AI in health should be treated as a context-sensitive system that must be tested, explained, and held accountable throughout its lifecycle.

4.6 Equity and Inclusion

App-based health systems risk deepening existing inequalities if they primarily serve digitally connected, literate, and formally documented populations while excluding those facing structural barriers to access. Rural communities, low-income groups, older persons, persons with disabilities, and individuals with limited digital literacy may be left behind when health services are delivered primarily through digital platforms. Equity must therefore be embedded in both the design and regulation of digital health systems.

This requires accessibility standards, multilingual interfaces where appropriate, low-bandwidth options, and offline alternatives in contexts with limited connectivity. It also requires attention to the datasets used to train and validate AI systems. African populations remain under-represented in many of these datasets, increasing the risk of biased or inaccurate outcomes. Regulators should therefore require validation across diverse African populations and ensure that digital health systems are designed to serve those who need them most, not only those already connected.

4.7 Accountability and Institutional Coordination

Effective governance of app-based health systems requires clear allocation of responsibilities across institutions, coordinated oversight mechanisms, and enforceable accountability frameworks. At present, responsibilities are often fragmented across health ministries, DPAs, and digital regulators, creating gaps in enforcement and uncertainty in regulatory oversight.

Regulatory frameworks should therefore clearly define institutional mandates and establish coordination mechanisms to ensure consistency in oversight, enforcement, and compliance monitoring. Developers and service providers should be subject to enforceable obligations, including breach notification requirements, audit duties, and liability for unlawful or discriminatory data practices. Strong institutional coordination is essential to ensure that regulatory frameworks are not only well-designed but also effectively implemented.

Where a health app exceeds a defined user threshold (such as 10,000 users), regulatory requirements should include the appointment of a Certified Health Data Officer (CHDO) to strengthen internal accountability and ensure compliance with data protection obligations. This would help prevent the illicit commercialisation of users' health data and reinforce data protection as a core condition for operating digital health services.

16 CIPESA, Submission to World Health Organization (WHO) on the Global Strategy on Digital Health 2028–2033, https://cipesa.org/wp-content/files/briefs/report/CIPESA_Submission_on_WHO_Digital_Health_Strategy.pdf

5. Conclusion

The endorsement of the Africa CDC Continental Health Data Governance Framework in February 2026 marks an important milestone, giving the continent a shared basis for active consent, interoperability, and secure cross-border health data flows. The task now is to translate those principles into national laws, institutional practice, and enforceable oversight mechanisms.

For African policymakers, the issue is not whether health data should move across borders, but under what conditions it should move, who should govern it, and how rights can be protected while public health and innovation are supported. Africa's health app ecosystem has already contributed to improved access, faster service delivery, and better coordination of care. Effective regulation will make that progress sustainable, accountable, and trustworthy.

Without appropriate safeguards, the same platforms that improve access can also expose sensitive data to misuse, commercial exploitation, and algorithmic discrimination. The recommendations below set out practical steps for regional institutions, governments, regulators, health providers, developers, and users to strengthen the governance of app-based health data and support a trusted digital health ecosystem across Africa.

6. Recommendations

African Union and Regional Bodies

- Support implementation of the Africa CDC Continental Health Data Governance Framework through clear timelines, monitoring mechanisms, knowledge-sharing platforms, and technical assistance for member states.
- Develop a continental health-app certification framework, recognised across participating jurisdictions, covering consent requirements, interoperability standards, cybersecurity safeguards, data governance obligations, and algorithmic accountability.
- Facilitate regional data trust zones through reciprocal recognition agreements among Data Protection Authorities, enabling secure and accountable cross-border health data flows for disease surveillance, research collaboration, and pandemic preparedness.

National Governments and Health Ministries

- Enact or strengthen health-specific data governance legislation that addresses the full data lifecycle in app-based health systems, including consent, purpose limitation, data minimisation, retention, breach notification, and cross-border transfers.
- Clarify institutional mandates by formally allocating oversight responsibilities across health ministries, DPAs, and digital regulators, and establish coordination mechanisms to reduce gaps and duplication.
- Require the registration and approval of health applications operating within national jurisdictions, with enhanced scrutiny for AI-enabled diagnostic, predictive, and clinical decision-support systems.
- Establish regulatory sandboxes to assess the safety, effectiveness, and governance implications of emerging digital health technologies before large-scale deployment.

Data Protection Authorities

- Conduct risk-based audits and impact assessments of high-impact health applications, including privacy, security, and algorithmic fairness where AI systems are deployed.
- Develop sector-specific guidance on the processing of health, biometric, and demographic data, including standards for research use, secondary use, and commercial processing.
- Enter into reciprocal recognition arrangements with counterpart DPAs across Africa to support coordinated enforcement and trusted cross-border data flows.
- Build specialised technical capacity to oversee AI-enabled health systems, algorithmic accountability requirements, and emerging digital health technologies.

Health Service Providers

- Migrate clinical records to certified Electronic Medical Record systems aligned with national interoperability requirements and recognised digital health standards.
- Formalise data processing agreements with health app vendors and third-party processors, including provisions on security, breach notification, audit rights, and liability.
- Strengthen workforce capacity through regular training on health data governance, cybersecurity, incident reporting, and the responsible handling of sensitive health information.
- Implement strong authentication, access-control, and encryption measures to protect patient information throughout its lifecycle.

App Developers and Platform Operators

- Embed privacy-by-design and security-by-design principles throughout the development, deployment, and operation of health applications.
- Provide clear and accessible consent mechanisms that enable users to understand and control how their health data is collected, shared, retained, and reused.
- Conduct regular testing and independent assessments of AI-enabled health tools to identify and address bias, accuracy concerns, and performance disparities across African populations.
- Comply with recognised interoperability standards and provide users with practical mechanisms to access, transfer, correct, and delete their personal data where permitted by law.
- Publish clear information about data sharing practices, automated decision-making systems, and relationships with third-party processors and partners.

Health Service Consumers and App Users

- Exercise rights over personal health data, including rights of access, correction, portability, and deletion where provided under applicable legal frameworks.
- Use health applications that comply with relevant regulatory requirements and recognised data protection standards.
- Report suspected data breaches, misuse of personal information, or harmful automated decision-making outcomes to relevant regulators and oversight bodies.
- Practise good digital hygiene, including the use of strong passwords, multi-factor authentication, and secure devices when accessing digital health services.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
+256 414 289 502
programmes@cipesa.org
@cipesaug facebook.com/cipesaug Linkedin/cipesa
www.cipesa.org