Policy **Brief**

What Does Kenya's Digital Health Act Portend for Data Governance and Regulation?

April **2024**

CIPESA

Introduction

Standardised, participatory and equitable access to quality healthcare services using ICT

The 2030 Agenda for Sustainable Development notes that the spread of Information and Communications Technology (ICT) and global interconnectedness have great potential to accelerate human progress, bridge the digital divide and develop knowledge societies.[1] However, according to the World Health Organization (WHO), despite advancements in technology, several countries are yet to fully realise the potential of digital health for positive health outcomes.[2] Untapped prospects include leveraging data and technology to devise interventions and solutions that improve health services delivery.[3]

Kenya has taken a step ahead in the East African region by enacting the Digital Health Act, 2023 following the Kenya National eHealth Policy 2016-2030.[4] The policy was built on the need for standardised, participatory and equitable access to quality healthcare services using ICT. The Act and the Policy, together with the Universal Healthcare Act, the Facility Improvement Financing Act and the Social Health Insurance Act,[5] aim to enhance access to quality, efficient, affordable and non-discriminatory healthcare.[6]

In addition, the Office of the Data Protection Commissioner (ODPC) has developed an extensive Guidance Note on the Processing of Health Data.[7] The Guidance aims to provide healthcare institutions with a clear understanding of their duties and obligations under the Data Protection Act, 2019. These measures show that Kenya is working to harness digital technologies to address healthcare challenges in the country including through the utilisation of technology and fostering effective management of health data.[8] This brief gives an analysis of the Digital Health Act and what it portends for health data governance in Kenya and possibly beyond.

1 *Adopted in United Nations General Assembly resolution 70/1 (2015).*

2 *World Health Organization, <https://www.who.int/health-topics/digital-health#tab=tab_1.*

3 *World Health Organization Global Strategy on digital health 2020-2025, https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf.*

4 *Kenya National eHealth Policy 2016-2030, https://repository.kippra.or.ke/bitstream/handle/123456789/1786/2016-2030%20Kenya%20National%20E-Health%20policy.pdf?sequence=1&isAllowed=y*

5 *NTV Kenya, In Photos: President Ruto signs four UHC Bills into law, https://ntvkenya.co.ke/news/in-photos-president-ruto-signs-four-uhc-bills-into-law/*

6 *President Ruto: New Healthcare Plan will leave no one behind, https://www.president.go.ke/president-ruto-new-healthcare-plan-will-leave-no-one-behind/.*

7 *Guidance Note on the Processing of Health Data, December 2023, https://www.odpc.go.ke/download/odpc-guidance-note-on-the-processing-of-health-data/?wpdmdl=9854&refresh=65b7d2c44d2551706545860*

8 *KELIN, Patient Empowerment, Innovation, Interoperability and Privacy: The Core of the Digital Health Bill 2023, https://www.kelinkenya.org/patient-empowerment-innovation-interoperability-and-privacy-the-core-of-the-digital-health-bill-2023/.*

What the Digital Health Act Promises

The Digital Health Act establishes a Digital Health Agency and a regulatory framework for the digital health ecosystem data life cycle and for e-waste management. It further aims to establish an integrated health information system; promote innovation and the safe, efficient and effective use of technology for healthcare; and enhance privacy, confidentiality and security of health data. It also provides for developing standards for provision of m-Health, telemedicine, and e-leaming; and provides for the safe and secure transfer of personal, identifiable health data and client's medical records to and from health facilities within and outside Kenya.[9]

Consequently, the enactment of this law could ensure more effective governance of health data. It presents an opportunity for strengthening patient data protection, as section 61 requires any person processing personal data under the Act to comply with the Data Protection Act, 2019. For much of Africa, existing data protection laws aim to generally protect data privacy. A dedicated digital health law, with compliance requirements under data protection regulation, is a positive step towards addressing the potential data privacy challenges related to health data.

If rightly implemented, the law will offer lessons in proper digital health data management and governance including in health data transfers, while also ensuring the rights of data subjects and the principles of data protection in the health sector are respected, protected, and promoted.

Exploratory Meaning of Terms

Given the novel nature of digital health in Africa and the evolving nature of technology, the Act defines various terms including those broadly related to data collection, processing, analysis and disposal. The Act goes a step further by defining terms at the intersection of data, technology and health service delivery. Among them are electronic health data, health data controller, health data custodian, health data processor, health informatics, health information bank, personal health information and research for health. If rightly applied, the definitions of the different terms will provide important guidance in understanding the multifaceted nature of digital health, health data management and governance.

9 *Digital Health Act, No. 15 of 2023, http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2015%20of%202023*

Guiding Principles for Health Data

Principles for data protection provide the basis for commitment to data protection. While general data protection regulations provide for the protection of individuals' personal data, health data presents unique features given its sensitivity. Health data is special and can be a basis for major threats, discrimination, harassment and surveillance.[10] Robust health data principles can thus guarantee protection of persons, groups of persons and the wider community.

Under section 4 of the Act, the principles to be followed in implementing the Act include treating health data as a strategic national asset, safeguarding privacy, confidentiality and security of health data for information sharing and use, facilitating data sharing and use for informed decision-making at all levels, and using the digital health eco-system to serve the health sector and to facilitate, in a progressive and equitable manner, the highest attainable standard of health.[11]

These principles could, while ensuring the progressive implementation of digital health solutions, guarantee privacy of individuals and groups of persons. However, if poorly managed and misused, discrimination based on gender and sexual identity, age, ethnicity and political inclinations could be perpetuated. This could hamper health service provision and delivery to sections of the population particularly those that are traditionally marginalised.

Establishment of the Digital Health Agency

The functions of the Digital Health Agency under section 6 of the Act include to develop, operationalise and maintain the comprehensive integrated health information system; promote health data portability and health data exchange; facilitate collection and analysis of data to inform policy and research in the health sector; spearhead health digitisation in the country; and and support the development and implementation of standards for enhanced interoperability.

There were concerns that since Kenya has an existing data protection authority - the ODPC - establishing the Digital Health Agency would lead to duplication of roles.[12] However, an independent agency dedicated to regulating health data is a positive step that will promote clear accountability and independent, sector-specific oversight. Health data presents complexities that require specific expertise and technical competencies in handling to ensure that privacy of patient information is guaranteed.

10 See for instance, Health Data Governance Principles, https://healthdataprinciples.org/principles (accessed November 27, 2023).

11 Section 4, Digital Health Act, 2023

12 David Indeje, Kenya's Digital Health Act: A Leap Forward in Data Governance, KICTANET, October 24, 2023, https://www.kictanet.or.ke/kenyas-digital-health-act-a-leap-forward-in-data-governance/ (accessed November 28, 2023).

An Integrated Health Information System

Sections 15 to 18 provide for the establishment of an integrated health information system which shall be administered by the Digital Health Agency. The Agency is a point of collection, collation, analysis, reporting, storage, usage, sharing, retrieval or archival of health data using all relevant ICT infrastructure to ensure quality assurance and data audits. Under section 18, the system shall be guided by data protection principles, scalability and interoperability, efficiency and effectiveness, simplicity and accessibility, and consistency.

Whereas the Digital Health Act may appear to repeat the need for an integrated approach to information systems that uphold the principles of privacy and data protection as outlined in the Data Protection Act, the emphasis on health information systems is commendable. In the past, there have been incidents of unlawful use of individuals' data within and outside of the health sector. For instance, during the surge of COVID-19, a number of countries such as Kenya and Uganda adopted measures to contain the virus but with very adverse impacts on data protection and privacy.[13] Moreover, there have been instances where governments have used health information to surveil individuals' movements and habits.[14] The Digital Health Agency must take all measures to ensure that the Integrated Health Information System robustly guards against unauthorised access, processing, use and transfer of individuals' private health information within the country as well as across its borders.

A Pace for Health Data Governance

Given the wide scope and sensitive nature of health data collected, such as in medical insurance, physician notes and diagnosis, medical records on current and past health history, health data governance that safeguards against breaches and misuse should be balanced with regulated access to inform disease surveillance, research and innovation.[15]

Section 19 of the Act classifies health data into several categories such as sensitive personal level health data; de-identified, pseudo-anonymised or anonymised individual-level health data; administrative data; aggregate health data; medical equipment data; and research for health data. This presents opportunities for easy categorisation and guidance in dealing with different types of health data. Furthermore, in laying down the data governing principles in section 20, including the minimisation of harm, data security, equity and accountability, privacy and confidentiality, as well as accuracy and reliability, the law reinforces the Data Protection Act which also provides for data protection principles. The categorisation of health data, stipulating the health data protection principles, and establishment of a health data governance framework in section 21, promote the effective use of health data.

13 *Surveillance, data protection, and freedom of expression in Kenya and Uganda during COVID-19, April 2021, https://www.article19.org/wp-content/uploads/2021/04/ADRF-Surveillance-Report-1.pdf*

14 *Reuters, False claim: Government 'uses virus' to control all aspects of citizens' lives, March 17, 2022, https://www.reuters.com/article/uk-factcheck-coronavirus-government-cont/false-claim-government-uses-virus-to-control-all-aspects-of-citizens-lives-idUSKBN2133U9/*

15 *KPMG, Data governance in healthcare, https://kpmg.com/xx/en/home/insights/2018/06/data-governance-driving-value-in-health.html*

Buttressing Confidentiality, Privacy and Security of Data

The Data Protection Act, 2019 is grounded on the need to protect data and information from unlawful breaches. It lays down the principles and obligations of personal data protection, the grounds for processing of sensitive personal data, and cross-border data transfers. Part V (sections 24 to 39) of the Digital Health Act buttresses these aspects by providing for confidentiality, privacy and security of data. These provisions emphasise the rights of the health data subjects, respect and protection of health data from unauthorised dealings, and creates responsibilities for controllers in the management of the health data bank. Moreover, section 30 provides for exceptional grounds under which sensitive personal data held in the system may be disclosed to a third party. The grounds include where the data subject is unable to give informed consent for the disclosure and such consent is given by a person authorised in writing by the data subject to grant consent.

Similarly, section 25 reiterates the principle of data retention and disposal. It provides for a minimum period of 20 years in the integrated health information system before health data can be disposed of except where the law requires otherwise or the retention has been authorised by the data subject or for historical, statistical or research purposes. Similarly, under section 25(3), the period beyond extension of the minimum period shall be secured by de-identification, anonymisation, pseudo–anonymisation or archiving, or establishing such technical and organisational security measures as the Cabinet Secretary may determine to be necessary.

The specification of the period for data retention and disposal of 20 years provides certainty on the period for which data should be retained. This overcomes the vagueness in the Data Protection Act which, under section 39, provides for retention “for as long as may be reasonably necessary for the purpose for which the personal data is processed”.

Facilitating Easy Access to, and Management of Health Services

Section 26 establishes National Health Data banks and spells out their roles and functions. A health data bank will be for data storage and facilitating integration and interoperability of the national health data bank with other relevant databases. By easing access to identification of patients and service providers, the health data banks will, among others, support decentralised care and treatment.

In section 27, the Act also emphasises the need for data collectors and processors such as health insurance providers and health facilities to take relevant measures and precautions when dealing with sensitive personal data. Nevertheless, some concerns may emerge especially in respect to conducting disease surveillance. In the past, disease surveillance, such as during the period of COVID-19 surge, saw the infringement of individuals' privacy, and their data was used for other purposes such as physical surveillance.[16] It is imperative to check against similar and other possible abuses of the data given the creation of a national health data bank and county health data banks.

E-Waste Management

Electronic waste raises environmental protection concerns since there are hardly clear regulations and guidelines in the developing world. While there are general Guidelines for E-Waste Management in Kenya,[17] implementation has been flawed. The Digital Health Act offers a glimpse of hope as it provides for management of e-waste in the health sector. Under section 45, e-waste management guidelines and a system will be developed in consultation with stakeholders and will comprise mechanisms for segregation, collection, transportation, and processing. This points to a positive direction in promoting the use of sustainable models for e-waste management through public -private partnerships.

It should, however, be noted that in promoting reuse and lifetime extension of e-waste in health data in section 45(2)(b), the law potentially creates opportunities where e-health data may be used unfairly by unscrupulous individuals for their own personal or selfish gain. The Cabinet Secretary should urgently develop guidelines which ensure that there is no opportunistic and unscrupulous re-use of e-health data. The guidelines should prescribe checks and limits of reuse. Moreover, data impact assessments should be the basis for any justifications of reuse and lifetime extensions.

16 *CIPESA, Health Data Regulation: Lessons from Covid-19 Surveillance in Kenya and Uganda, 2023, https://cipesa.org/wp-content/files/briefs/Health_Data_Regulation-_Lessons_from_COVID-19_Surveillance_in_Kenya_and_Uganda_Brief.pdf*

17 *Guidelines for E-Waste Management in Kenya, 2010, https://www.nema.go.ke/images/Docs/Guidelines/E-Waste%20Guidelines.pdf*

Conclusion

The Digital Health Act is a progressive move towards appropriate regulation of digital health services in Kenya. It points to the relevance of technology in enhancing health care. There is a clear thread of provisions which are fundamentally inclined towards rights-respecting data governance in the health sector, alongside support for research and innovation. However, health data is highly sensitive and e-health and e-health data management are in nascent stages in the country. Proactive education of service providers and citizens, as well as robust enforcement of the Act, will be critical in enabling the new law to engender effective data governance and improved health services delivery.

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