



**Transform
Health**
KENYA



Legislative Guide:
**DIGITAL HEALTH
TECHNOLOGIES AND
DATA IN KENYA**

**LEGISLATIVE GUIDE:
DIGITAL HEALTH TECHNOLOGIES AND DATA
IN KENYA**



Table of Contents

LIST OF ACRONYMS.....	6
ACKNOWLEDGEMENT.....	7
INTRODUCTION.....	8
DEFINITION OF TERMS.....	10
 1. GENERAL PRINCIPLES.....	 11
2. RECOMMENDED LEGISLATIVE ISSUES ON DIGITAL HEALTH.....	16
i) Background: Perspectives of global and international agencies.....	17
ii) Basis for development of digital health legislation in Kenya.....	20
iii) Recommended legal and policy actions:.....	20
(a) Digital Health Systems.....	20
(b) Hardware for Digital Health.....	21
(c) Digital Health Software Services.....	21
(d) Digital Health Technologiess.....	21
(e) Network and Connectivity.....	22
(f) Communication Interface.....	22
(g) Privacy, Confidentiality, Security and Medical Ethics.....	22
(h) Digital Health Ethics.....	23
(i) Interoperability.....	23
(j) Data Sharing.....	24
(k) Standardization.....	24
(l) Governance.....	24
(m) Dispute Resolution.....	24
(n) Operationalization.....	25
 ANNEX 1: SUMMARY OF GUIDING LEGISLATIVE AND POLICY ENVIRONMENT.....	 26
ANNEX 2: ANNEX 2: UNIVERSAL HEALTH COVERAGE POLICY 2020 – 2030: RECOMMENDED ACTIONS RELATING TO DIGITAL HEALTH.....	36
ANNEX 3: SUMMARY OF E-HEALTH REGULATIONS IN THE UK AND US.....	38
ANNEX 4: ESSENTIAL REQUIREMENTS FOR E-HEALTH SYSTEMS IN THE EU.....	41

Abbreviations and Acronyms

CR	:	Client Registry
DCHNI	:	Digital Health Care Northern Ireland
DHCW	:	Digital Health and Care Wales
eCHIS	:	Electronic Community Health Information System
EHDS	:	European Health Data Space
EHR	:	Electronic Health Record
FDA	:	Food and Drug Administration
HIE	:	Health Information Exchange
HIS	:	Health Information System
ICS	:	Integrated Care System
ICT	:	Information Communication Technology
IOT	:	Internet of Things
KELIN	:	Kenya Legal & Ethical Issues Network on HIV and AIDS
KEMRII	:	Kenya Medical Research Institute
KHIS	:	Kenya Health Information System
KIPRA	:	Kenya Institute of Public Policy Research and Analysis
LGDO	:	Local Government Digital Office
MoH	:	Ministry of Health
MPI	:	Master Patient Index
NACOSTI	:	National Commission for Science, Technology and Innovation
NGO	:	Non-Governmental Organisations
NUPI	:	National Unique Patient Identifier
PHR	:	Personal Health Record
PMA	:	Premarket Approval Application
SaMD	:	Software as a Medical Device
TPLC	:	Total Product Lifecycle
TS	:	Terminology Service
UK	:	United Kingdom
US	:	United States

Acknowledgement

Transform Health Kenya appreciates the valuable contributions by the consultants, Senaji Associates, who led the drafting and development of this guide. We are also grateful to all coalition partners who reviewed the guide and provided vital input and comments that helped shape the contents of the guide. The partners include Kenya Health Informatics Association (KeHIA); White Ribbon Alliance (WRA Kenya); Key Populations Consortium (KP Consortium); Love Matters Kenya; Partners for Health and Development in Africa (PHDA), Youth Alive Kenya, Pictures Youth Group, HealthX Africa, Nelson Mandela TB HIV Information CBO, Young Experts: Tech 4 Health (YET4H), Men for Positive Living Support CBO. We also appreciate the Centre for Intellectual Property and Information Technology Law (CIPIT) for support in review of the guide.

Transform Health Kenya appreciates the Kenya Legal and Ethical Issues Network on HIV and AIDS (KELIN) for coordinating the development of the guide. Particular appreciation to the project team: Timothy Wafula (Programme Manager, Health & Governance) and Martha Ogutu (Programme Officer, Health & Governance) for their invaluable support in development of the guide.

This report is published with technical and financial support from Transform Health.





Introduction


Transform Health Kenya, in line with Transform Health Global, commissioned the development of this guide through the Kenya Legal & Ethical Issues Network on HIV and AIDS (KELIN), its national coordinator. The guide aims to support the development of laws and policies on e-health technologies at both national and county level.

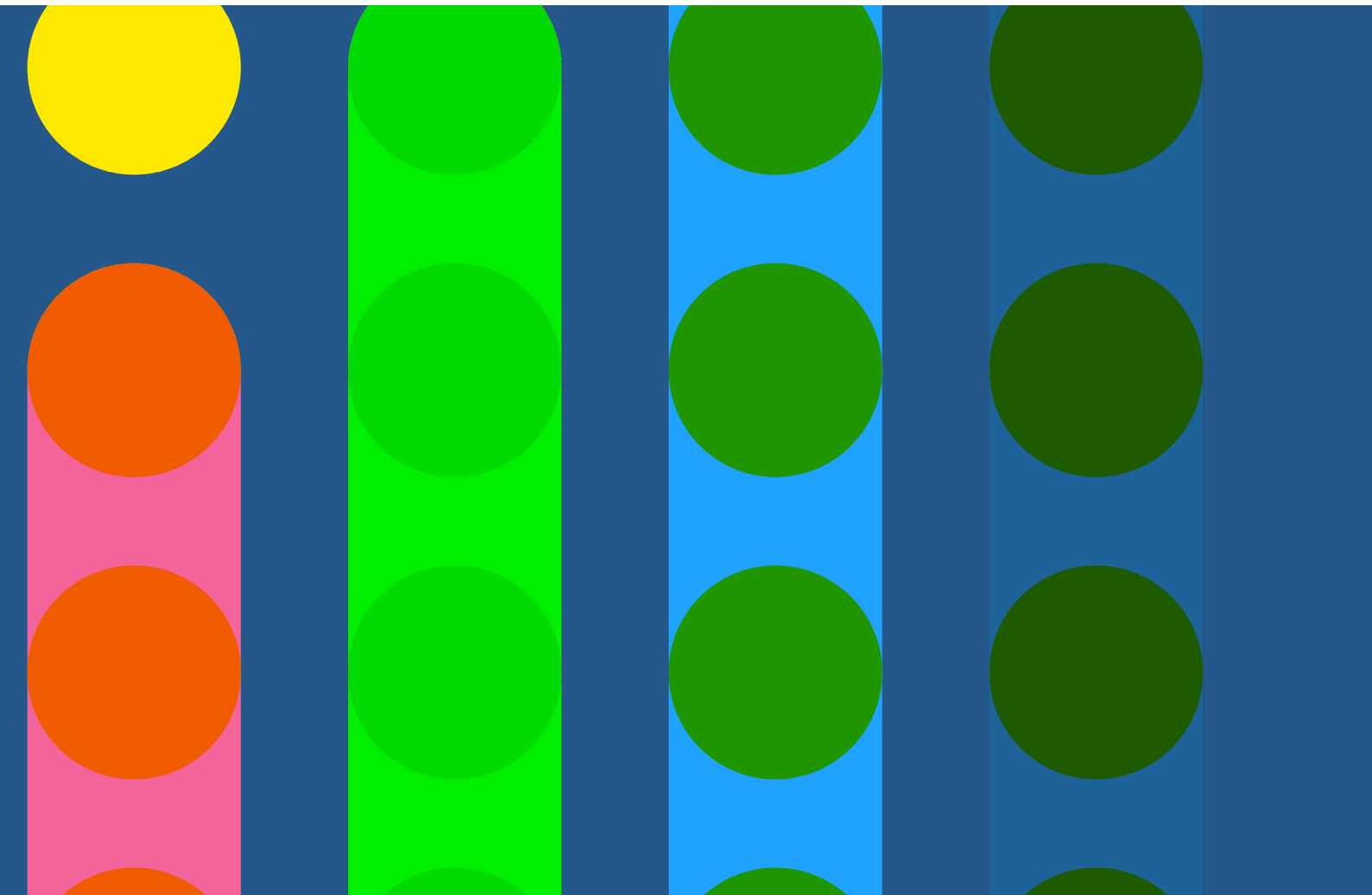
The guide is a summation of a consultative process involving health sector stakeholders and proposes progressive interventions to promote the objectives envisioned under the Health Act 2017, more specifically provide a roadmap for the realization of Sections 104(a), (b), (c), (d), (f) and (g) relating to e-legislation.

Additionally, the guide is informed by a mapping of existing legal and policy frameworks in the health sector in Kenya and supplemented by a consideration of health legal and policy frameworks from other jurisdictions i.e the EU, UK and US for the purposes of developing substantive and distinct recommendations.

This guide is developed in the strong belief that:

Solving professional health care services delivery deficiencies can best be accomplished with e-health standards, the specifications that enable interoperability among healthcare-related information and communication technologies and systems made by different





providers. Standards represent information in common formats, encrypt or compress information, perform functions like error detection and correction, or provide common addressing or security structures. All these functions, taken together, are what enable the reliable and interoperable sharing of information over communication networks and between devices that adhere to these common standards.

In order to respond more effectively to the growing burden of chronic disease, lack of health records, lack of health facilities in remote areas, poor road infrastructure, and other health sector challenges there is need to address problems such as poor coordination of rapidly expanding pilot projects, fragmented health services, a lack of awareness and education about digital health, unstable electricity supply, poor internet access, and the communication gap of the various digital health systems are limiting digital health implementation in Africa. [These are just but a few examples that continue to exist because of lack of effective implementation of government policies, legislations and regulation, weak governance and leadership and inadequate funding].

It is envisaged that this guide will guide further efforts towards improving the conditions for e-health in Kenya as an enabler towards achievement of the Universal Health Coverage commitments.

Definition of Terms:

In this guide:

Competent Authority: Entity mandated to regulate or oversee provision and enforcement of digital health services.

Digital Health: Digital health is the field of knowledge and practice associated with the development and use of digital technologies to improve health. Digital health expands the concept of eHealth to include digital consumers, with a wider range of smart devices and connected equipment. The following areas are commonly understood as being part of, or related to, digital health: artificial intelligence, big data, blockchain, health data, health information systems, the infodemic, the Internet of Things, interoperability and telemedicine.¹

Digital Health Systems Systems: designed to both generate and apply evidence to promote innovation, quality, safety and efficiency in health care.²

e-health: the combined use of electronic communication and information technology in the health sector including telemedicine;³

Broadly it means,

“the cost-effective and secure use of information and communications technologies in support of health and health-related fields, including health-care services, health surveillance, health literature, and health education, knowledge and research.”⁴ It encompasses multiple interventions, including tele-health, telemedicine, mobile health (mHealth), electronic medical or health records (eMR/eHR), big data, wearables, artificial intelligence and digital health.

Key Entities: include healthcare providers and other entities that lawfully hold a natural person’s health data and/or information

Software as a Medical Device: means software intended for one or more medical uses including diagnosis, mitigation, treatment, and prevention of disease that may run on different operating systems or in virtual environments without being part of a hardware medical device;

Total Conversation Service: means an audiovisual conversation service providing bidirectional symmetric real-time transfer of motion video, text, and voice between users in two or more location.

¹https://www.who.int/europe/health-topics/digital-health#tab=tab_1

²<https://bmcmmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-019-1005-7#:~:text=The%20Institute%20of%20Medicine%20views,health%20care%E2%80%9D%20%5B35%5D.>

³Per the Health Act No.21 of 2017

⁴<https://www.emro.who.int/health-topics/ehealth/>



PART 1

GENERAL PRINCIPLES



The following principles should guide the design of all laws, policies and guidelines on e-health or digital health:

A. National values and principles of governance under Article 10 of the Constitution including participation of the people; human dignity, equity, social justice, inclusiveness, equality, human rights, non-discrimination, protection of the marginalised; among others.

B. Respect, protection, promotion and fulfilment of rights and fundamental freedoms in the Bill of Rights, including:

- Article 43 (1) (a) of the Constitution that provides for every person to have the right to the highest attainable standard of health, which includes the right to health care services.
- Article 31 that provides for every individual to have the right to not have the information relating to their family and private affairs unnecessarily revealed.

- Article 35 where every citizen has the right to access information held by the State and held by another person and required for the exercise or protection of another right.

C. Principles of data protection provided for under section 25 of the Data Protection Act, 2019, as follows:

- processing of data in accordance with the right to privacy.
- processing of data lawfully, fairly and in a transparent manner.
- collection of data only for explicit, specified, and legitimate purposes and no further processing in a manner incompatible with those purposes.
- adequate, relevant, limited to what is necessary in relation to the purposes for which data is processed.
- collected only where a valid explanation is provided whenever information relating to family or private affairs is required.
- accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate

personal data is erased or rectified without delay.

- kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
- not transferred outside Kenya unless there is proof of adequate data protection safeguards or consent from the data subject.

D. Rights of the data subject provided under section 26 of the Data Protection Act, which are;

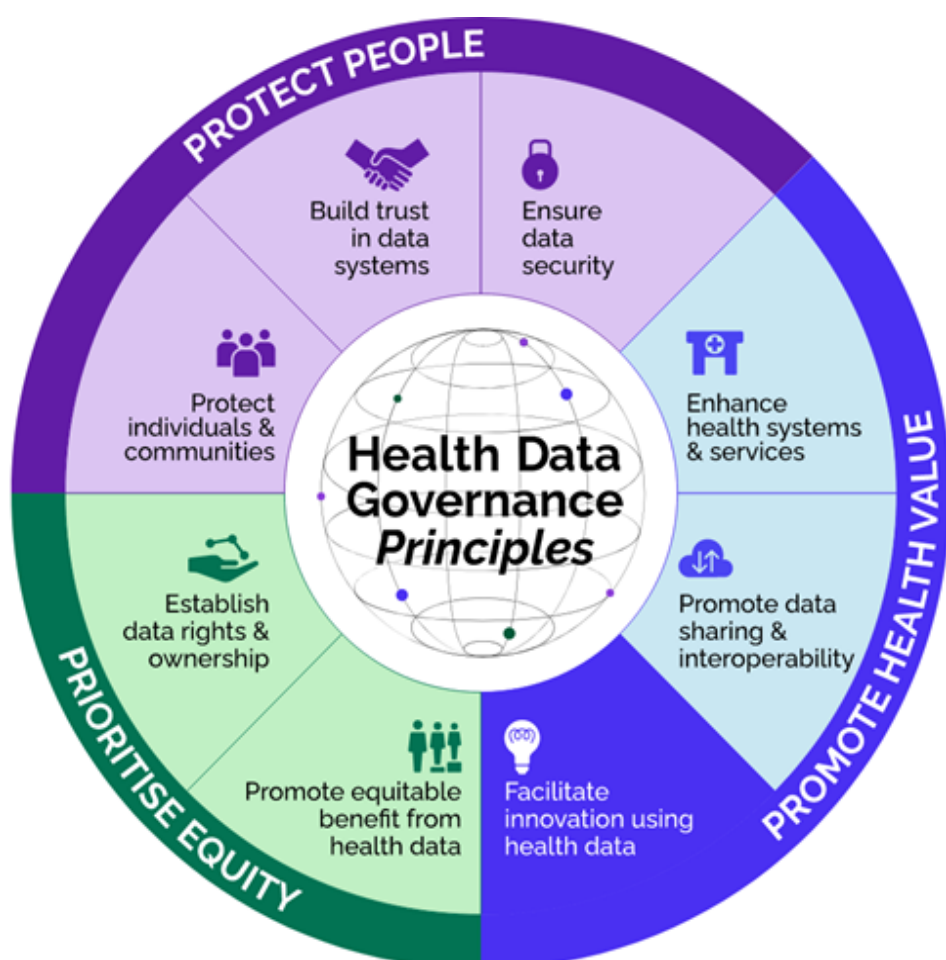
- The right to be informed of the use to which their personal data is to be put;
- The right to access their personal data in custody of data controller or data processor;
- The right to object to the processing of all or part of their personal data;
- The right to correction of false or misleading data; and
- The right to deletion of false or misleading data about them.

E. Global Health Data Governance Principles. Transform Health stewarded the development of the following 8 Health Data Governance Principles:

No.	Health Data Governance principle	Core Elements
1.	Protect Individuals and Communities	<ul style="list-style-type: none"> • Address individual and collective risk • Collect data with a defined purpose. • Collect personal or sensitive data only when necessary and with informed consent. • Use secure data collection and storage mechanisms. • Use de-identification and anonymisation • Define inappropriate uses of health data. • Institute safeguards against discrimination, stigma, harassment and bias. • Provide guidance specific to marginalised groups and populations.
2.	Build Trust in Data Systems	<ul style="list-style-type: none"> • Align with best practices for data protection and privacy. • Ensure consent is informed and understood in all its complexities. • Obtain collective consent where appropriate. • Define concrete exceptions to informed consent. • Ensure data quality, availability, and accessibility. • Reinforce health data governance with evidence. • Establish transparent and accessible processes and systems. • Institute feedback and accountability mechanisms.

No.	Health Data Governance principle	Core Elements
3.	Ensure Data Security	<ul style="list-style-type: none"> Require strong technical security measures for data processing. Mitigate risks related to security threats. Ensure transparency around data breaches. Consider federated data systems
4.	Enhance Health Systems and Services	<ul style="list-style-type: none"> Evaluate the benefits of health data. Use data to enhance health services for individuals and communities. Encourage a culture of data-led insights and action. Address health system efficiency, effectiveness, and resilience Strengthen community ownership of health data. Enable and empower frontline health workers
5.	Promote Data Sharing and Interoperability	<ul style="list-style-type: none"> Establish data sharing rules and guidelines. Validate informed consent before sharing data. Promote interoperability of data systems Define common data structures across health systems. Define multiple levels of data access. Use common definitions and global standards. Support multi-sector partnerships
6.	Facilitate Innovation Using Health Data	<ul style="list-style-type: none"> Apply health data governance to emerging technologies. Address the use of non-health data in health contexts. Build public health data infrastructure. Employ policy innovation
7.	Promote Equitable Benefits from Health Data	<ul style="list-style-type: none"> Represent all groups and populations equitably in data. Consider the unique needs of marginalised groups and populations. Mitigate data bias. Use accessible language and plug knowledge gaps. Implement inclusive data feedback mechanisms. Promote equitable impact and benefit

No.	Health Data Governance principle	Core Elements
8.	Establish Data Rights and Ownership	<ul style="list-style-type: none"> • Apply a human rights lens to health data governance. • Define clear governance roles and responsibilities. • Codify data rights and ownership. • Extend data rights and ownership to products and services. • Develop health data trusts and health data cooperatives. • Employ participatory data governance mechanisms. • Connect to broader accountability mechanisms



Pictorial representation of Health Data Governance Principles



PART 2

RECOMMENDED LEGISLATIVE ISSUES ON DIGITAL HEALTH



i. Background: Perspectives of global and international agencies

The World Health Organization (WHO) 2020-2025 Global Strategy on Digital Health notes four guiding principles aimed towards appropriate and sustainable adoption of Digital Technologies within the context of national health sector and health strategies. The four principles;

- Acknowledge that institutionalization of digital health in the national health system requires a decision and commitment by countries.
- Recognize that successful digital health initiatives require an integrated strategy
- Promote the appropriate use of digital technologies for health and
- Recognize the urgent need to address the major impediments faced by least-developed countries implementing digital health technologies.

In recognizing the need for an integrated strategy for digital health initiatives, the

WHO notes the importance of such strategies being led through strong governance structures. Objective 3 of the Global strategy further focuses on strengthening governance for digital health at global, regional and national levels and specifically calls for the creation of sustainable and robust governance structures and building the capacity for digital health at global and national levels. It promotes standards for safety, security, privacy, interoperability, and the ethical use of data within and outside the health sector. Actions to strengthen governance should include defining principles and reaching cross-sectoral and international agreements for data sharing, quality and accuracy of health data and prioritization of investment plans and policy. It should also include principles for the ethical use of health data in technologies such as artificial intelligence and big data analytics.⁵

The World Bank observes that the ability to uniquely identify patients across healthcare facilities can improve administration,

⁵<https://www.who.int/docs/default-source/documents/gsdhdaa2a9f352b0445bafbc79ca799dce4d.pdf>

patient management, and the quality of care by ensuring that individuals can be repeatedly and correctly identified when accessing services throughout the country (UNAIDS 2014, WHO 2012, WHO 2017a). When combined with an EHR system, a unique identifier facilitates a longitudinal history for each patient, including health status, diagnoses, test results, treatments, and outcomes over time. This reduces administrative duplication, wasted resources, and potentially dangerous errors in medications, transfusions, and testing (WHO 2007).⁶

The World Health Organization (WHO)⁷ in relation to policy, legislation and

compliance recommends that countries should put in place systems to ensure data privacy, ownership, access, integrity and protection of patient information and rigorously **ensure** that these systems meet national legal standards, the concerns of clients and that health workers, clients and other stakeholders are aware of and able to use these systems.

It also recommends rolling out programmes that account for the inequities in programme design, and proactively develop and implement alternative means of providing services to those who would be left out by digital only and other inequities.

Prioritization of needs of vulnerable populations:

Particular attention needs to be paid to the needs, preferences and circumstances of particularly disadvantaged or hard-to-reach groups, including people with low literacy or digital literacy skills, people speaking minority languages, migrant populations in new settings, people affected by emergency situations, or people with disabilities such as sight or hearing impairment.

Source: WHO

Digital health technologies should not deliberately or unintentionally discriminate against individuals. Moreover, to ensure equity in implementation, these technologies should account for the needs of vulnerable and marginalized groups, including women, children, racial and ethnic minorities, migrants, people living with HIV and other key populations. Effective, non-digital options should also be available and accessible to all.

Source: UNDP

UNDP⁸ observes that the adoption of national digital health strategies can facilitate coordination, set standards for interoperability, and establish policies related to digital health and for identifying gaps and opportunities where digital technologies can be best leveraged to improve health outcomes. These strategies should be developed in a consultative

and transparent manner that accounts for the needs of vulnerable and marginalised communities and those living in urban, rural, crisis, and conflict settings, should have political support from a variety of different stakeholders and should undergo periodic reviews to ensure relevance and recognize the rapid evolution of digital health technologies.

⁶<https://documents1.worldbank.org/curated/en/595741519657604541/pdf/The-Role-of-Digital-Identification-for-Healthcare-The-Emerging-Use-Cases.pdf>

⁷<https://www.who.int/publications/i/item/9789241550505>

⁸undp.org/sites/g/files/zskgke326/files/2021-07/UNDP-Guidance-on-the-rights-based-and-ethical-use-of-digital-technologies-in-HIV-and-health-programmes-2-EN.pdf

The African Union (AU) Digital Transformation Strategy (2020-2030),⁹ identifies digital health as one of the critical approaches in driving a digitally transformed continent for prosperity and inclusivity. Digital platforms are also an essential element of digital infrastructure and can serve people in all aspects of life including healthcare. The Strategy encourages governments to entrust national start-ups and social enterprises with public projects by adopting their cost-efficient solutions to address local issues among which include health. Urges Member States to establish robust monitoring and evaluation frameworks and harmonise key performance indicator (KPI) frameworks across digital health initiatives to support realisation of the full potential of digital health.

Further, the Africa CDC, intends to advocate and provide Member States with guidance on creating a legal and regulatory framework that allows National Public Health Institutes, researchers, and private sector to use health data in a trusted and secure way.¹⁰ This is aimed at fostering digital market innovation.

It is also noted that when countries routinely develop and maintain their own shared digital platforms, resources can be more efficiently allocated, and public health officials, practitioners, and decision-makers can make informed decisions across all areas of service delivery, sectors, and public health in ways that improve demand and risk forecasting, support tracking of individual patients, and help to identify and respond to disease outbreaks and other public health threats.¹¹

The EU recommends that to scale up research and innovation and better enable personalised solutions, digital health service

providers should demonstrate data sharing collaborations with industry data spaces to improve the design, monitoring, post market surveillance and predictive maintenance of medical devices and equipment installed in health care provider organisations.¹²

Achieving effective shared digital platforms requires a coordinated approach from all global health partners and sectors, where global, regional, and local use cases are accounted for as part of the design and implementation of digital health systems, and the data generated from these systems are used by a competent, capable workforce to inform local service delivery, global and regional health activities, science research and policy

Source: CDC

To support efficacious interventions for priority populations, the USAID recommends developing community Health Information System (HIS), such as electronic case management information systems Supporting electronic medical records systems that track and monitor client data at health facilities to assure quality client care and improved treatment outcomes and rollout of national and subnational data and analytics platforms to support health program decision-makers in visualising integrated data sets and using a standardised approach to analyse and action data in real time for continuous program improvement.¹³ The Global Fund recommends expanding the range of platforms for service delivery, and delivering integrated, people-centred services.¹⁴

⁹<https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf> ¹⁰<https://www.who.int/publications/i/item/9789241550505>

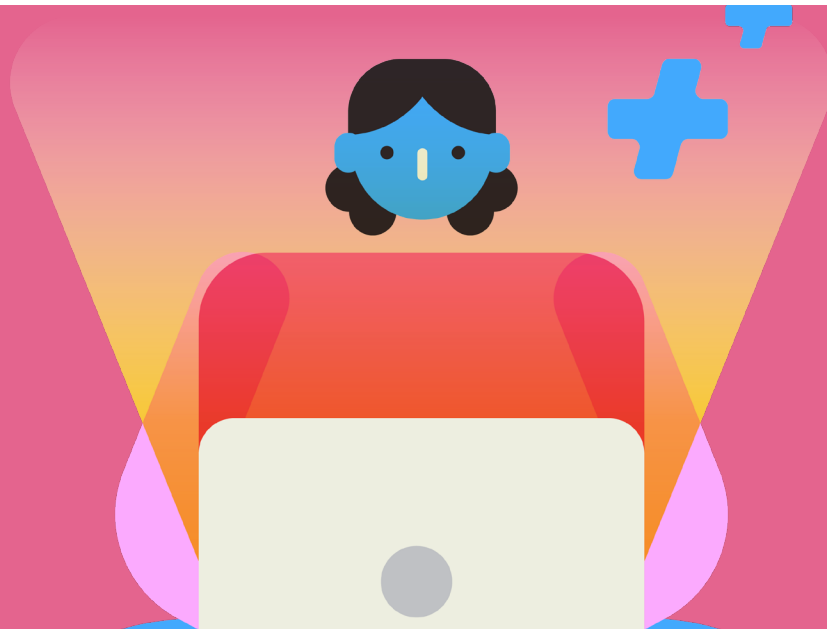
¹⁰<https://africacdc.org/wp-content/uploads/2022/12/Africa-CDC-DTS-Summary-for-CPHIA-3.pdf>

¹¹https://www.cdc.gov/globalhealth/topics/gdhs/pdf/GDHS_Strategy2022_REV_508.pdf

¹²https://digitalhealtheurope.eu/wp-content/uploads/DHE_recommendations_on_EHDS_July_2021.pdf

¹³<https://www.usaid.gov/global-health/health-areas/hiv-and-aids/technical-areas/using-health-information>

¹⁴https://www.theglobalfund.org/media/4794/core_keypopulations_technicalbrief_en.pdf



ii. Basis for development of digital health legislation in Kenya

Section 104 Health Act, 2017 mandates the Cabinet Secretary Ministry of Health, within three years of the operation of the Act, to ensure the enactment of legislation that provides for among other things—

- a. administration of health information banks including interoperability framework, data interchange and security
- b. collection and use of personal health information
- c. management of disclosure of personal health information.
- d. protection of privacy
- e. business continuity, emergency, and disaster preparedness
- f. health service delivery through M-health, E-learning, and telemedicine
- g. E-waste disposal
- h. health tourism

iii. Recommended legal and policy actions:

1. Digital Health Systems

- a. The Government should ensure that the national and county digital health systems are interoperable as to enable connection of components with central data repositories where different healthcare processing services within the system can securely access and update patient records.
- b. Digital health systems should be able to accommodate “occasionally connected” systems where data is stored locally and connected to a central repository periodically when the internet is available.
- c. Digital health systems should include secure storage of patient history on alternative technologies such as smartcards to allow health record portability across different healthcare services in areas with no internet connectivity.
- d. Digital Health solution providers should invest in the development of big data technologies with regards to storage and transmission of health information in public/national/county data centres to facilitate access to data to promote the development of new digital health services and applications.

2. Hardware for Digital Health

- a. The procurement of digital health technologies should be done in accordance with prevailing procurement laws and should be accompanied by appropriate maintenance and service agreements.
- b. Digital health technologies should conform to pre-development functional specifications and guarantee fitness for purpose, quality, and reliability.
- c. Hardware used in the provision of digital health services should at their end of life be recycled through flexible take-back plans involving collaboration with private sector.
- d. Manufacturers of digital health technologies should embrace continuous product testing improvements based on lessons learned from previous projects, research and consumer needs to provide responsive solutions for provision of digital health.

3. Digital Health Software Services

- a. Digital health software contracts should include information on the software requirement specifications, source code availability, payment plans for phased milestone-based solutions, software documentation including installation and user manuals, modification and update particulars, warranty on compliance with applicable national legislation.
- b. The Ministry of Health or designated relevant authority should maintain a register of all digital health systems that are developed, tested, piloted, or implemented in the national and county healthcare institutions.
- c. All healthcare sector software should conform to the national or Ministry of Health approved Digital Architecture & Interoperability Standards unless otherwise excluded by a relevant competent authority.

- d. National and County healthcare facilities should only use appropriately licensed software including for free and open-source software.
- e. Where software is donated to the national or county governments, no vendor lock-in should be permitted.
- f. The piloting of software systems or their component(s) should be done at selected institutions accompanied by proper evaluation of the pilot project and where the pilot involves a third party, the evaluation should be done independent of the third party.

4. Digital Health Technologies

- a. Data driven technologies should be transparent, safe, accountable, and effective and should guarantee the privacy of data subjects.
- b. Digital health technologies must be clinically safe to use and must comply with National clinical safety standards including in the manufacture and deployment of technologies.
- c. Digital health processes and data should be made open to inspection by publishing information about the project or technologies in complete, open, understandable, easily accessible, and free formats.
- d. Digital health project technology cycles should have effective governance and oversight mechanisms that enable effective public scrutiny.
- e. Digital health technology project cycles should eliminate unintended discriminatory effects on individuals, mitigate biases and ensure that the technologies respect the dignity of individuals, are just, non-discriminatory, and consistent with the public interest, including human rights and democratic values.
- f. Digital health products and services should be designed to deliver better and responsive healthcare solutions characterized by value proposition

based on inclusive research on user needs across the entire product lifecycle. / Digital health technologies should be leveraged in the development of products and services designed to deliver better and responsive healthcare solutions characterised by value propositions based on inclusive research on user needs across the entire product lifecycle.

- g. Digital health technology providers should ensure that their products are easy to use and accessible to all users.
- h. Digital health technologies should be appropriately tested and fit for purpose based on assurance plans that define testing approaches and specify how technologies will continue to be developed and managed.
- i. Digital health technologies must be clinically safe to use and must comply with National clinical safety standards including in the manufacture and deployment of technologies.
- j. Digital health technologies should utilise open standards to maximise data quality and interoperability, with the goal of providing access to all.
- k. Digital Health Technologies providers should invest in solutions that provide better energy efficiency, embrace of usage of alternative and renewable resources, and reduce carbon emissions to reduce adverse environmental impacts.

5. Network and Connectivity

- a. Government should implement policy and regulatory measures that facilitate deployment and use of digital health technologies for affordable digital health infrastructure and services, including in infrastructure sharing, interconnectivity, quality of service and access.
- b. The government and competent authorities should promote open network protocols and technology neutrality subject to applicable minimum standards to ensure freedom of hardware selection.

- c. Digital Health supply-side stakeholders should continuously provide solutions that guarantee business continuity and emergency and disaster preparedness and 'always on and available' secure access to quality e-health services.

6. Communication Interface

- a. Health Information Systems providers should adopt security solutions that enable secure conveyancing for both direct and indirect communications over HIS interfaces that support authentication of users and guarantee confidentiality of sensitive data.
- b. Patient portals should be secure spaces that give patients access to their personal health information and enable secure messaging with healthcare providers and should continuously be reviewed to improve quality of care.
- c. Digital health technologies should support total conversation services to provide efficient real time conversation for all people and for varying situations including people living with disabilities, e.g. the deaf or hard of hearing, blind and people who find themselves in a situation where the complementing media video, real-time text and voice together fulfill the conversation needs much better than only voice.
- d. Personally Identifiable and Login Authentication Credentials should be encrypted using the appropriate algorithms.

7. Privacy, Confidentiality, Security and Medical Ethics

- a. National and County Governments, healthcare institutions and organizations must implement policies that ensure that health information is secure in line with provisions of the Data Protection Act and only used or accessed by authorized individuals appropriately.
- b. Healthcare stakeholders should adopt and implement technologies such as

block chain among other developing technologies that support secure information exchange, transaction validation and identity management.

- c. Key entities must ensure that health information is properly protected while allowing the flow of health information needed to provide and promote high-quality healthcare, and to protect the public's health and well-being and should rely on professional ethics and best judgment when considering requests for these permissive uses and disclosures.
- d. Key entities and other digital health service providers offering e-health services to consumers should adopt appropriate technical and organizational security standards including voluntary standards necessary to guarantee the safety of consumers and integrity of patient data.
- e. Digital health service providers should guarantee consumer privacy by ensuring that their practices relating to the collection and use of consumer data are lawful, transparent and fair, minimal, enable consumer participation and choice, cognizant of all data subjects' rights and provide reasonable security safeguards.
- f. Digital Health systems should be designed with events (security) logs that allow tracing of successful and failed log-in attempts.
- g. Medical Ethics: Ensuring the privacy and confidentiality of digital healthcare consumers should be paramount in all digital Health solutions.

8. Digital Health Ethics

- a. The government in consultation with stakeholders should assess the ethical issues arising with the use of digital health technologies and in line with continued technological advancements develop relevant frameworks, guides, and policy that address the arising ethical issues.
- b. The government should develop the

infrastructure necessary for vetting new digital health technologies before undertaking any implementation processes.

- c. Government should ensure that digital health technologies deployed and implemented do not further widen the digital divide. Digital health technologies must not be a source for discrimination in the access to health care.
- d. Government and private sector Implementation strategies prior to deployment of digital health technologies should provide and require adherence with ethical concepts and principles in the implementation processes to protect and prevent the end user/ consumer from exploitation.

9. Interoperability

- a. The digital health ecosystem should have the ability of different information systems, devices, and applications (systems) to access, exchange, integrate and cooperatively use data in a coordinated manner, within and across organizational, regional and national boundaries, to provide timely and seamless portability of information and optimize the health of individuals and populations globally to include foundational, structural, semantic and organizational interoperability.
- b. Digital health software should allow uniform and consistent sharing of health information across any application.
- c. Digital health applications should ensure interoperability among the institutional systems exchanging health information, and guarantee compatibility among medical devices and digital systems, regardless of manufacturer.
- d. Interoperability of data health systems should be characterized by findable, accessible, interoperable, and reusable data to improve patient access, foster portability, and promote safety and transparency.

10. Data Sharing

- a. The health information sharing systems should facilitate access to and retrieval of clinical data by key stakeholders and provide safe, timely, efficient, effective, and equitable patient-centred care.
- b. Health Information System providers should maintain consent management policies that enable users and patients to effectively regulate access to their health information including like opt-in, opt-out and secondary use protocols.
- c. Health institutions should establish secure information sharing mechanisms where health information can be lawfully accessed, authenticated, and utilized in the provision of legitimate health services.
- d. Health institution, in their role as data controllers and processors must ensure that they adhere to the provisions on the Data Protection Act, 2019 and the Data Protection General regulations, 2021 on sharing of data.

11. Standardization

- a. The government should ensure secure, confidential, quality, interoperable and ethical aggregation of health data into public health data repositories for limited and lawful use in health research.
- b. The government should promote adoption of practical and implementable standards including for patient summaries, ePrescriptions/eDispensations, laboratory reports, medical images and reports and hospital discharge reports.
- c. The government or the Ministry of Health shall specify the international and/or regional standards to be used for provision of the respective digital health services and solutions.
- d. The government and competent authorities should ensure early adoption and consistent implementation of key digital health standards and should

promote uniform application of applicable standards across providers.

12. Governance

- a. Stakeholders including National and County Governments should collaborate to promote uptake and effective use of digital health services across the country, particularly in rural and remote areas, through incentives that are attractive to both the public and private sectors to support universal health coverage obligations.
- b. Government in collaboration with stakeholders in the health sector should consider adopting enabling and innovative regulatory approaches to support further research in digital health such as regulatory sandboxes to test new technology, start up and experiment interfaces to support experimental initiatives, pilot projects to obtain initial feedback and facilitate reflection and design of future digital health solutions and promoting further public participation and consultation in the regulatory process. Stakeholders should raise awareness on the benefits of digital health transformation and support its adoption across all populations indiscriminately.
- c. Government should localize decision making to gain crucial insights for (re)shaping a comprehensive policy framework as well as business decisions based on local contexts in either part or all of Material, Use, and End-of-Life stages of a digital health technology product or service from all major stakeholders including policy makers, industry executives, consumers and general citizens.

13. Dispute Resolution

- a. Consumers of digital health services should be provided with meaningful access to fair, easy-to-use, transparent,

and effective mechanisms to resolve e-health disputes in a timely manner and obtain redress, as appropriate, without incurring unnecessary cost or burden.

- b. Digital health services platforms should have internal complaints handling mechanisms, which enable consumers to informally resolve their complaints directly with providers, at the earliest possible stage, without charge.
- c. Digital health service providers should ensure that the dispute resolution mechanisms comply with the following minimum standards; accessibility; accountability; competence, confidentiality; equality; impartiality; legality; security; and, transparency.

14. Operationalization

The National and County Governments should;

- a. Designate national and county authorities to oversee implementation.
- b. Collaborate and establish a database of licensed e-health service providers collaborating with public health institutions accessible to consumers.
- c. Harmonize standards on secure and interoperable health information exchange across health institutions;
- d. Cooperate to monitor, evaluate, and report on the implementation of e-health; and,
- e. Enhance the capacity of public health institutions to serve as an enabler of e-health within the Universal Health Coverage Obligations.



PART 3

ANNEXURES

Annex 1: Summary of guiding legislative and policy environment

Law/Policy	Description	Implications for Digital Health
Constitution, 2010	<p>Article 43 (1) (a) of the Constitution provides that every person has the right to the highest attainable standard of health, which includes the right to health care services.</p> <p>Article 31: Every individual has the right to not have the information relating to their family and private affairs unnecessarily revealed.</p> <p>Article 35. Every citizen has the right to access information held by the State and held by another person and required for the exercise or protection of another right.</p>	Provides for pursuit of progressive and sustainable health services interventions and guarantees protection of health information.
Health Act, No. 21 of 2017 ¹⁵	Enacted to establish a unified health system, to coordinate the inter-relationship between the national government and county government health systems, to provide for regulation of health care service and health care service providers, health products and health technologies and for connected purpose.	<p>Defines:</p> <p>“e-Health” as the combined use of electronic communication and information technology in the health sector including telemedicine;</p> <p>“health technology” refers to the application of organized knowledge and skills in the form of devices, medicine, vaccines, procedures and systems developed to solve a health problem and improve the quality of life</p> <p>“telemedicine” refers to the provision of health care services and sharing of medical knowledge over distance using telecommunications and it includes consultative, diagnostic, and treatment services</p> <p>Provides for the fundamental duty of</p>

¹⁵<http://kenyalaw.org/8181/exist/kenyalex/actview.xql?actid=No.%2021%20of%202017>

Law/Policy	Description	Implications for Digital Health
		<p>the State to observe, respect, protect, promote and fulfil the right to the highest attainable standard of health including reproductive health care and emergency medical treatment by inter alia ensuring the prioritization and adequate investment in research for health to promote technology and innovation in health care delivery; [S. 4(b)].</p> <p>Mandates the National Government to regulate health products and health technologies including assessment, licensing and control of commercial and industrial activities; [S. 24(d)];</p> <p>Provides for the Regulation of Health Products and Technologies [Part VII]</p>
Pharmacy and Poisons Act ¹⁶	Establishes the Pharmacy and Poisons Board responsible for the regulation of health products, technologies, and the profession of pharmacy	<p>Defines:</p> <p>“medical device” as any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article-</p> <p>a) intended by the manufacturer to be used, alone or in combination, for humans or animals for diagnosis, prevention, monitoring, treatment or alleviation of disease; diagnosis, monitoring, treatment, alleviation of or compensation for an injury; investigation, replacement, modification or support of the anatomy or of a physiological process; supporting or sustaining life; control of conception; disinfection of medical devices; or providing information for medical or diagnostic purposes by means of in vitro examination of specimens derived from the human body; and</p>

¹⁶<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=CAP.%20244>

Law/Policy	Description	Implications for Digital Health
		<p>b) which does not achieve its primary intended action in or on the human or animal body by pharmacological, immunological or metabolic means, but which may be assisted in its intended function by such means;</p> <p>“health technology” as the application of organized knowledge and skills in the form of devices, medicine, vaccines, procedures and systems developed to solve a health problem and improve the quality of life;</p>
Access to Information Act, No. 31 of 2016 ¹⁷	Section 3(d): Enacted to promote routine and systematic information disclosure by public entities and private bodies on constitutional principles relating to accountability, transparency and public participation and access to information.	a public entity or private body may be required to disclose information where the public interest in disclosure outweighs the harm to protected interests as shall be determined by a Court with due regard to constitutional principles including to keep the public adequately informed about the existence of any danger to public health or safety or to the environment.
Data Protection Act, No. 24 of 2019 ¹⁸	<p>Sections 25, 31, and 46 of the Act regulates collection, processing, storage, and retention of sensitive personal data and protects privacy of data subjects in line with the constitution.</p> <p>Regulates collection, processing, storage, and retention of sensitive personal data while defining principles and obligation of personal data protection.</p>	<p>Defines “health data” as data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services.</p> <p>Empowers the Data Commissioner to develop sector specific guidelines in consultation with relevant stakeholders in areas such as health, financial services, education, social Protection and any other area as the Data Commissioner may determine. [S. 74(1)(d)].</p>

¹⁷<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2031%20of%202016>

¹⁸<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019>

Law/Policy	Description	Implications for Digital Health
	Provides for the processing of personal data relating to health by or under the responsibility of a health care provider; or by a person subject to the obligation of professional secrecy under any law. [S. 46]	
Kenya Information and Communication Act, No. 2 of 1998 ¹⁹	Provides for the regulation of electronic data as legal data. Section 83(G) defines Electronic records as legal records. Section 83(H) provides for period Retention of electronic Records. Section 83(I) requires retention of information in original form.	Guides how data collected will be stored and archived. Specifically, the provisions that guide database architecture that ensures availability of data as collected. Provides for ancillary regulation of the information society such as infrastructure sharing, technology standards, internet connectivity and communication services.
Computer Misuse and cybercrime Act, No.5 of 2018 ²⁰	Enacted to provide for offences relating to computer systems; to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes; to facilitate international co-operation in dealing with computer and cybercrime matters; and for connected purposes. The Act aims at protection of confidentiality, integrity and availability of computer systems, programs, and data. It also requires information sharing and auditing of information infrastructure.	Defines “critical infrastructure” as the processes, systems, facilities, technologies, networks, assets and services essentials to the health, safety, security or economic well-being of Kenyans and the effective functioning of Government. Mandates the auditing of critical information infrastructure - to check for compliance Information sharing for authorized persons.

¹⁹<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%202%20of%201998>

²⁰<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%205%20of%202018>

Law/Policy	Description	Implications for Digital Health
Health Records and Information Managers Act, No.15 of 2016 ²¹	Enacted to make provision for the training, registration and licensing of the health records and information managers; to regulate their practice; to provide for the establishment, powers and functions of the Health Records and Information Managers Board and for connected purposes.	<p>Defines “Manager” as an officer trained in health records and information and charged with the responsibility of managing health records and information for health services which include: consulting in clinical coding, coding for insurance firms, capacity building in disease classifications and health information management, appraisal of medical documentations and audit, medical data analytics and research, use of e-health applications, development of strategic documents and policies in health records and information management services, advice on medical legal issues, advice on retrieval and disposal of medical records, management of bed bureaus or consultancy in administrative statistics and big data analytics.</p> <p>Mandates the Health Records and Information Managers Board to, among others, establish and improve the standards of professional health records and information management in Kenya; [S. 6(1)(b)].</p>
Pharmacy and Poisons (Registration of Health Products and Technologies) Rules, 2022 ²²	Regulation of health products and technologies	A person shall not import, manufacture, or sell a health product or technology in Kenya unless that health product or technology has been registered under the Pharmacy and Poisons (Registration of Health Products and Technologies) Rules, 2022.

²¹<http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2015%20of%202016>

²²<http://www.parliament.go.ke/sites/default/files/2022-10/Legal%20Notice%20No.%20100%20of%202022%20relating%20to%20the%20Pharmacy%20and%20Poisons%20%28Registration%20of%20Health%20Products%20and%20Technologies%29%20Rules%2C%202022%20and%20the%20Explanatory%20Memorandum%20from%20the%20Ministry%20of%20Health.pdf>

Law/Policy	Description	Implications for Digital Health
Kenya National E-Health Policy 2016 - 2030	Policy with a vision to create an enabling environment for the sustainable adoption, implementation and efficient use of e-health products and services at all levels of healthcare delivery in Kenya.	<p>The country's e-health framework revolves around three strategic objectives contained in the policy;</p> <p>(i) The need to enhance interaction between client and health service provider, through promoting electronic access to quality healthcare by establishing interaction platforms between the client and health service providers; enabling health service providers and their clients to easily collaborate and consult each other electronically; improving client-provider interaction through ICTs; and promoting clients' decision making and management of their health.</p> <p>(ii) The need to accelerate achievement of universal health coverage, through improving health literacy levels by providing materials to patients on how to use e-health, promoting availability, accessibility and affordability of ICT infrastructure, devices and connectivity and ensuring deployment of user-friendly e-health platforms for ease of use.</p> <p>(iii) The need to enhance electronic exchange of health data and information, through ensuring standardization of stored data to promote interoperability of e-health systems; continuous improvement of infrastructure and resources to support cost effective implementation of tele-health applications and ensuring prompt and convenient access to patient's demographic and clinical data to privileged healthcare providers.</p> <p>Guiding principle 3.1.3 of the National e-Health Policy acknowledges that appropriate standards for e-health hardware and software is a requirement as is standardization of</p>

Law/Policy	Description	Implications for Digital Health
		<p>procurement of e-health solutions to ensure quality, confidentiality, privacy, security, and the integrity of health data. In the policy, it is noted that:</p> <p>One of the challenges to the adoption of e-health is the lack of standards and guidelines that are localized to the context of use. This has forced most e-health product and service providers to opt for proprietary standards from developed countries that may not be applicable in Kenya.</p>
Kenya Primary Health Care Strategic Framework 2019-2024	Describes how primary healthcare reporting should be handled. Gives a Description of Primary Health Care Networks.	Primary health care facilities data should reflect the health of the catchment population not just those seeking. Minimum functional requirements for service delivery and reporting are based on this framework.
Community Health Strategy 2020-2025	This strategy gives priority areas of focus in community health including information for the period 2020/2025	Provision for social accountability and how this information will be collected using the community score card which can be digitized. It also points out what is envisioned in terms of community health information system.
Standards and Guidelines for electronic records systems	Coordination of development, deployment, implementation, and maintenance of these Systems.	This document provides guidance on the approach to be adopted in development, deployment, implementation, and the maintenance of the Electronic Community Health Information. System (eCHIS).
Kenya Standards for e-health Interoperability 2020	Provides guidance on integration of systems.	This framework provides guidance on how to link health information to other HIS platforms within Ministry of Health (MOH).

Law/Policy	Description	Implications for Digital Health
Kenya Health Sector Data Quality Assurance Protocol, 2014	Data Quality improvement strategies.	Defines procedures for DQA during implementation of e-health.
National Integrated data analytics	Data analysis towards tracking indicators and informing policy.	Sets a framework for the establishment of data visualization and analytic tools.
Kenya Standards and Guidelines for mHealth systems, 2017	Design and development of mHealth solutions.	<p>Outlines the development of the various domains, mHealth applications that support and exchange data for e-health.</p> <p>Cover the legal and ethical concerns in the mHealth application development and implementation including the liability of the community health volunteer in the data transmitted from the mobile device, involve the sharing of client data, shared confidentiality, transmission of the data over wireless connections, and data encryption considerations.</p>
Kenya Standards and Guidelines for E-Health Systems Interoperability ²³	To provide and promote use of highly effective, reliable, and innovative information systems to support clinical decision making, patient management, and health care research to improve health care services in Kenya.	Provides the key principles for e-health interoperability standards and acknowledges the role of international data exchange standards in inter alia, enabling the Kenya health sector to be more effectively operated as an interconnected system, overcoming the current fragmentation and duplication of service delivery.
Core Standards for Quality Healthcare ²⁴	Framework is aimed at providing the necessary guidance to inform unique patient identification strategies that will ultimately facilitate higher quality healthcare services for all Kenyans.	Dimension 9 provides for Health Records and Health Management Information Systems to support the delivery of safe and effective services.

²³https://pdf.usaid.gov/pdf_docs/PA00TB28.pdf

²⁴https://www.health.go.ke/wp-content/uploads/2021/10/KQMH-Quality-Standards-Final-Booklet_March-2018.pdf

Law/Policy	Description	Implications for Digital Health
Health Sector Unique Identification Framework 2022 ²⁵	Framework is aimed at providing the necessary guidance to inform unique patient identification strategies that will ultimately facilitate higher quality healthcare services for all Kenyans.	Establishing the Unique Patient Identification (UPI) is a crucial step toward the development of Health Information Exchange (HIE), which will enable data sharing between various systems within the health sector. This framework help lay the foundation for HIE in Kenya including - <i>uniquely identifying patients for the collection and retrieval of the necessary information to deliver optimum health care (e.g., diagnosis, treatment, blood transfusion, medication)</i>
National Community Health Digitization Strategy 2020-2025	This strategy document provides a digitization blueprint that will support a comprehensive approach to community health service delivery.	Envisages the development of a national electronic Community Health Information System (eCHIS) to respond to the gaps identified in community health service delivery and data management through the eCHIS Landscape Assessment and intensive stakeholder engagement ²⁶ .

²⁵<https://www.health.go.ke/wp-content/uploads/2022/09/Health-Sector-Unique-Identification-Framework-30-August-2022.pdf>

²⁶<https://www.health.go.ke/wp-content/uploads/2021/03/eCHIS-Strategy-2020-2025.pdf>

Annex 2: Universal Health Coverage Policy 2020 – 2030: recommended actions relating to digital health:

	Component	Gap/Action Area
Kenya UHC Policy 2020-2030 ²⁷	<u>Service Delivery</u> Enhancing the quality of care and services provided - 2.3.3 (ii)	To enhance the quality of care and services provided in public and private health facilities, the national Quality of Care Certification Framework for the Kenyan Health Sector 2020 should be implemented to ensure a harmonised registration, licensing, and certification process that facilitates continuous quality improvement. This will also enhance ease of doing business, medical tourism, and strategic purchasing of health services.
	<u>Health Products and Technologies (HPTs)</u> Improving access to priority health products and technologies - 2.3.5 (i)	Accurate forecasting and quantification at facility, County and National level is important to enhancing availability of priority health products and technologies. There is need to strengthen capacity to ensure forecasting and quantification is done every two years as guided by national guidelines. The capacity of the Kenya Medical Supplies Agency and other registered pooled purchasers of HPTs should be strengthened to ensure optimal pricing and improved quality and availability of HPTs and efficiency of operation.
	<u>Health Information Systems</u> Optimising the use of information to improve health systems performance - 2.3.6 (i)	Data from Health Information System (HIS) is not optimally utilised for priority setting, allocation of resources and informed decision making at all levels. The Kenya Health Information System (KHIS) has made significant gains in its ability to provide data collected routinely. However, the information system remains fragmented with gaps resulting from inadequate utilisation of existing data platforms e.g., poor linkage of information on clinical episodes with financial systems, parallel systems for vertical programs, poor linkage with other data systems (e.g., civil registration) and poor private sector participation. Existing platforms continue to display gaps in the completeness, quality, and timeliness of data. There remain gaps in the capacity to analyse and utilize data

²⁷<https://www.health.go.ke/wp-content/uploads/2022/02/UHC-POLICY-2020-2030-FINAL.pdf>

	Component	Gap/Action Area
		<p>for decision making, more so at the point of care. While a policy framework has been developed for health information systems and related technologies, its implementation remains inadequate with challenges in uniformity, interoperability, and security. There is need for digitization of the HIS to obtain real time data for informed decisions at all levels.</p> <p>Finally, there is a need to address the patient's role in information systems, particularly as concerns ownership of data and its portability particularly to enhance patient rights, safety, and care.</p>
	<u>Health Infrastructure</u> Address persistent gaps in and optimise use of existing health infrastructure - 2.3.7 (i)	<p>There has been an increase in health infrastructure through both public and private investments. Physical access to health services is inadequate and the standards not optimal as prescribed in the Infrastructure Norms and Standards. Distribution of health facilities remains disparate geographically, with concentration of health service providers in urban areas.</p>
	<u>Research and Development</u> Strengthening the link between research, policy and implementation - 2.3.8 (i)	<p>The Ministry of Health (MOH) has made strides in enhancing its generation and utilisation of research by publishing its National Health Research Priorities, establishing the National Research Committee and establishing the Kenya Health and Research Observatory. The MOH works closely with National Commission for Science, Technology and Innovation (NACOSTI), the Kenya Institute of Public Policy Research and Analysis (KIPPRA), the Kenya Medical Research Institute (KEMRI), universities and other research and learning institutions to enhance evidence - informed policymaking and strengthen ethical conduct of research. Key challenges remaining are inadequate levels of domestic funding for research in health and the institutionalization of evidence - informed practice at all levels including in training, clinical care and in priority setting.</p>

Annex 3: Summary of e-health regulations in the UK and US

	UK	USA
Regulation	<p>Health and Social Care Act, 2008²⁸ defines “Health care” to include all forms of health care provided for individuals, whether relating to physical or mental health, and also includes procedures that are similar to forms of medical or surgical care but are not provided in connection with a medical condition.</p> <p>Human Medicines Regulations, 2012²⁹ defines “medicinal product” as -</p> <ul style="list-style-type: none"> a) any substance or combination of substances presented as having properties of preventing or treating disease in human beings; or b) any substance or combination of substances that may be used by or administered to human beings with a view to— <ul style="list-style-type: none"> (i) restoring, correcting or modifying a physiological function by exerting a pharmacological, immunological or metabolic action, or (ii) making a medical diagnosis. <p>Medical Devices Regulations, 2002³⁰ provides that no person shall place on the market or put into service a relevant device unless that device meets the essential requirements under the Regulations.</p>	<p>Health Insurance Portability and Accountability Act, 1996 establishes national standards to protect individuals’ medical records and other personal health information.</p> <p>Health Information Technology for Economic and Clinical Health Act, 2009 – enacted to promote the adoption and meaningful use of health information technology.</p> <p>Federal Food, Drug and Cosmetic Act, 1938 - authorizes the Food and Drug Administration (FDA) to oversee and regulate the production, sale, and distribution of food, drugs, medical devices, and cosmetics.</p>

²⁸<https://www.legislation.gov.uk/ukpga/2008/14/contents>

²⁹<https://www.legislation.gov.uk/uksi/2012/1916/regulation/2/made>

³⁰<https://www.legislation.gov.uk/uksi/2002/618/regulation/8/made>

	UK	USA
	<p><u>General Regulations</u></p> <p>General Data Protection Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.³¹</p> <p>Data Protection Act, 2018³² sets out how personal data must be collected, handled and stored to protect people's privacy</p> <p>Electronic Commerce Regulations, 2002</p> <p>Consumer Rights Act, 2015</p> <p>Consumer Protection from Unfair Trading Regulations, 2008</p>	
Regulatory Authority	<p>Care Quality Commission (England)</p> <p>Healthcare Improvement Scotland</p> <p>Care Inspectorate Wales</p> <p>The Regulation and Quality Improvement Authority (Northern Ireland)</p>	Department of Health and Human Services – General Health and Safety .
	<p>The Medicines and Healthcare Product Regulatory Agency</p>	
<hr/> <p>³¹https://gdpr-info.eu/art-1-gdpr/</p> <p>³²https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted</p>		

	UK	USA
Digital Health Technologies	<ul style="list-style-type: none"> • Digitised Health Systems • mHealth • Telemedicine • Health Data Analytics 	<ul style="list-style-type: none"> • Telemedicine/Virtual Care, • Robotics, • Wearables, • Virtual Assistants, • mHealth/Mobile Apps, • Software as a Medical Device (SaMD), • Clinical Decision Support Software, • Artificial Intelligence/Machine Learning powered digital health solutions, • Internet of Things (IOT) and connected devices, • 3D Printing/Bioprinting, • Digital Therapeutics, • Natural Language Processing

Annex 4: Essential requirements for e-health systems in the EU³³

Requirement	Component	Gap/Action Area
General Requirements	Fitness for Purpose	An Electronic Health Record system (EHR system) shall achieve the performance intended by its manufacturer and shall be designed and manufactured in such a way that, during normal conditions of use, it is suitable for its intended purpose and its use does not put at risk patient safety.
	Compatibility	An EHR system shall be designed and developed in such a way that it can be supplied and installed, taking into account the instructions and information provided by the manufacturer, without adversely affecting its characteristics and performance during its intended use.
	Rights-centered	An EHR system shall be designed and developed in such a way that its interoperability, safety and security features uphold the rights of natural persons, in line with the intended purpose of the EHR system.
	Security	An EHR system that is intended to be operated together with other products, including medical devices, shall be designed and manufactured in such a way that interoperability and compatibility are reliable and secure, and personal electronic health data can be shared between the device and the EHR system.
Interoperability Requirements	Data Sharing	An EHR system shall allow personal electronic health data to be shared between health professionals or other entities from the health system, and between health professionals and patient or health professional portals in a commonly used electronic interoperable format.

³³https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_2&format=PDF

Requirement	Component	Gap/Action Area
Security Requirements	Security by Design	An EHR system shall be designed and developed in such a way that it ensures safe and secure processing of electronic health data, and that it prevents unauthorized access to such data.
	Accountability	An EHR system designed to be used by health professionals shall provide reliable mechanisms for the identification and authentication of health professionals, including checks on professional rights and qualifications.
	Access Limitation	An EHR system shall include tools and mechanism to allow natural persons to restrict health professionals' access to their personal electronic health data but shall also include mechanisms that allow access to personal electronic health data in emergency situations, and ensure that access is strictly logged.
	Data Retention	An EHR system designed for the storage of electronic health data shall support different retention periods and access rights that consider the origins and categories of electronic health data.



**Transform
Health**
KENYA