REPUBLIC OF KENYA

MINISTRY OF HEALTH

KENYA HEALTH DATA GOVERNANCE FRAMEWORK

2025

MINISTRY OF HEALTH

KENYA HEALTH DATA GOVERNANCE FRAMEWORK 2025

A trusted health data ecosystem

Suggested citation: Ministry of Health, Kenya. Kenya Health Data Governance Framework; 2025.

Ministry of Health
P.O. Box: 30016–00100, Nairobi.
Afya House, Cathedral Road
+254-20-2717077

www.health.go.ke

Table of Contents

Chapter 4 - Health Data Leadership, Governance and Operations

Chapter 5 - Health Data Management

Chapter 6 - Implementation Plan

Chapter 7 - Monitoring, Evaluation and Learning

List of Tables and Figures

List of Tables

List of Figures

FOREWORD

Every Kenyan has a constitutional right to the highest attainable standard of health. The Government of Kenya is committed to delivering this through the implementation of Universal Health Coverage (UHC). This will give Kenyans access to an affordable standard package of healthcare services on demand. UHC will be implemented on a foundation of primary health care, supported by four pillars that address human resources for health; financing; health products and technologies; and health information.

Delivery of quality health care depends on the availability of real-time quality data within the health ecosystem at the right time and to the right person for decision making at all levels. The expansion and transformation of technology has contributed to the recognition of digital health as a powerful catalyst for delivering universal health coverage, under the caption “Leave no one behind”.

As a result, the Ministry of Health is spearheading the digitisation of Kenya’s health ecosystem and utilising lessons learnt from various digital health implementation initiatives that have taken place in Kenya over the past three decades, developing shared common resources to enable the interoperability and integration of the various electronic systems within the ecosystem. This pursues the objective of a comprehensive and integrated health information system, as envisioned by the Health Act, 2017 and established by the Digital Health Act, 2023.

With the increasing use of technology comes the urgent need to ensure that health data is optimally governed and meets the key principles of data governance, namely: protection of people’s data; equity; and increasing the value of data through its use at all levels. A strengthened legislative and policy environment will facilitate digitisation within the health sector. The Ministry of Health has therefore developed the Kenya Health Data Governance Framework as a guide that ensures that health data, within the comprehensive and integrated health information system, is grounded on internationally accepted health data governance principles and complies with existing legislation including the Data Protection Act, 2019 and the Digital Health Act, 2023.

It is my sincere hope that all who interact with health data at various levels of the health ecosystem will find the Kenya Health Data Governance Framework useful as we all work towards meeting its overall vision of “A trusted health data ecosystem”!

Hon. Aden Duale, EGH
Cabinet Secretary,
Ministry of Health

ACKNOWLEDGMENTS

The development of the Kenya Health Data Governance Framework is the result of determined concerted efforts from many individuals and organisations. The process was inclusive and participatory, and utilised the latest content, expertise and best practices in health data governance.

We offer special thanks for the dedicated support from the offices of the Cabinet Secretary and Principal Secretaries for the overall stewardship. Sincere gratitude goes to Dr Patrick Amoth, Director General for Health, for his strategic guidance throughout the process. We acknowledge the support of the Council of Governors in coordinating the participation of counties in the process of developing this Framework.

The Ministry acknowledges the contributions of the data governance and health informatics technical working groups and the health information research, monitoring, and evaluation inter-coordinating committee co-chaired by Dr. Ayub Manya, Head of the Directorate of Digital Health, Health Informatics, Research and Policy, and Dr. Greg Ganda, County Executive Committee Member (CECM) - Health, Kisumu County. The MoH acknowledges the role of Dr. Joseph Sitienei in initiating the process of development of this Framework, the continued support of Dr. Bernard Langat in guiding its evolution, and subsequent completion under the able leadership of Dr. Ayub Manya. We also recognize the dedication of the technical lead, Dr. Joyce Wamicwe, whose collaboration with Pascal Mwele, Dr. Jacob Odhiambo, and Evans Munene from Palladium-Kenya, as well as George Owiso from the University of Washington, and Dr. Ramona Koech from the Tony Blair Institute for Global Change, was invaluable. Special thanks go to Steven Wanyee, engaged as a consultant through the Tony Blair Institute for Global Change, for his significant contributions to the process. We acknowledge Eng. Antony Lenaiyara, CEO Digital Health Agency, and the various reviewers for their input at various stages of the development of this Framework.

Specific acknowledgements go to Palladium Data Modernization Initiative Project and Centers for Disease Control and Prevention, Kenya for the financial and technical support provided throughout the development of this Framework. A list of all contributors is provided in the annex section of this Framework. To everyone we say a big “Thank You”!

In conclusion, we are confident that this Framework will inform the process of the establishment of health data governance in the country with the promotion of the inherent value of this data being realised. We therefore call upon all state and non-state actors to utilize this Framework fully as we all work towards meeting its overall vision: “A trusted health data ecosystem”.

Dr. Ouma Oluga, OGW,
Principal Secretary,
State Department for Medical Services

Mary Muthoni, CBS,
Principal Secretary,
State Department for Public Health and Professional Standards

EXECUTIVE SUMMARY

Kenya's ongoing digital transformation of the health sector has generated unprecedented volumes of health data, creating new opportunities for improved service delivery while also amplifying risks around privacy, security, and accountability. The Health Data Governance Framework (HDGF) provides a unifying structure for addressing these challenges by grounding health data governance in constitutional principles, statutory mandates, and coordinated sector oversight.

The Framework is anchored in the Constitution of Kenya (2010), which places direct obligations on the State to ensure: the right to privacy (Article 31), the right to access information (Article 35), and the right to the highest attainable standard of health (Article 43). These provisions situate health data governance firmly within Kenya's broader system of public administration, intergovernmental coordination, and health sector accountability. The HDGF translates these constitutional commitments into practical mechanisms that strengthen the leadership and oversight roles of both the Ministry of Health (MoH) and county governments as costewards of the health system.

The Framework aligns with key national laws including the Data Protection Act (2019), the Health Act (2017), and the Digital Health Act (2023). The Digital Health Act specifically establishes the Digital Health Agency (DHA) as the national Health Data Custodian, responsible for maintaining the Comprehensive Integrated Health Information System (CIHIS), ensuring secure interoperability, and enforcing national data governance standards. DHA implements Kenya's digital health architecture, working under the policy direction of the Ministry of Health and in close coordination with county governments.

Chapter 3 identifies persistent governance gaps including fragmented systems, weak interoperability, uneven capacity, inconsistent consent practices, and variable data quality. The Framework contextualises global principles of transparency, privacy, security, and equity to Kenya's legal and operational environment, ensuring that governance practices reflect both international norms and the realities of a devolved system.

The HDGF is its explicit delineation of leadership, coordination, and oversight roles across the national and county levels, as described in Chapter 4. The Ministry of Health, as the national steward of policy, regulation, and health sector strategy, is responsible for setting standards, issuing guidelines, coordinating national oversight platforms, and ensuring the uniform interpretation and implementation of health data governance laws. The MoH also provides national-level stewardship for system design, regulatory harmonisation, and cross-sectoral coordination, ensuring that health data governance aligns with Kenya's broader digital transformation agenda and national health priorities.

County governments as constitutionally mandated to deliver health services, play an equally crucial role. The Framework reinforces the accountability of County Executive Committee Members (CECMs) for Health, who serve as county-level data controllers. Counties are responsible for managing County Health Data Banks, enforcing compliance with national standards, appointing Data Protection Officers, ensuring adherence to data sharing and access protocols, and driving facility-level implementation. Their oversight directly affects the accuracy, security, and integrity of routine service data, making county leadership essential for operationalising the Framework in frontline service settings.

Chapter 5 translates these roles into operational guidance across the health data lifecycle, ensuring that data collection, validation, processing, sharing, retention, and disposal adhere to constitutional protections, statutory requirements, and sector standards. These lifecycle requirements strengthen nationalcounty coordination by clarifying “who does what” at every stage of data handling, thereby reducing fragmentation and reinforcing accountability.

The Implementation Plan (Chapter 6) outlines a phased approach that begins with establishing governance structures, followed by nationwide capacitation of MoH and county teams, and culminating in scaled adoption across all health facilities. Throughout these phases, the MoH provides strategic direction and national harmonisation, while counties lead local implementation, workforce readiness, and system routine use. Chapter 7 introduces a Monitoring, Evaluation, and Learning (MEL) framework that enables national and county actors to track progress, assess compliance, and adapt governance approaches as technologies and health needs evolve.

This document represents Kenya resolve to build a trusted, secure, and equitable health data ecosystem that enhances service delivery, strengthens public confidence, and drives innovation across both national and county health systems.

Dr. Patrick Amoth, CBS
Director General for Health

DEFINITION OF KEY TERMS

Term	Definition
Anonymisation	Removal of all identifiers from personal data so that the data subject is no longer identifiable as per the Data Protection Act, 2019
Data registry	A collection of standardised information about a group of individuals
Data use	The optimal application of data, including evidence, facts, figures, and statistics generated from it, by a group of people or organisation, to inform their
Data value chain	A series of processes that include collection, storage, processing, sharing, archiving, and disposing data. Activities in each of those stages define and enable derivation of value from interaction with the data in that stage
Digital Exhaust Data:	This is the trail of digital data generated by a user's interactions with digital devices which includes but not limited to information about a patient's, equipment functioning and utilization, logs etc
Electronic Health Record	A repository of information regarding the health status of a subject of care, in computer processable form
Electronic Medical Record	A computerised legal medical record created by organisations delivering health care, such as clinics and hospitals. Electronic medical records tend to be a part of the health information system, allowing for the storage, retrieval and manipulation of records.

Health data	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
Health ecosystem	A healthcare ecosystem consists of the people, organisations, medical knowledge, practices, protocols and rules, technologies, standards and regulations that govern health operations.
Health record	A compilation of an individual's health information including all past and present medical conditions, illnesses and treatments and their overall health status.
Identifiable natural person	A person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity as per the Data Protection Act, 2019
Paraclinical	Relating to branches of medicine that provide a service to patients without direct involvement in clinical care
Personal data	Any information relating to an identified or identifiable natural person as per the Data Protection Act, 2019
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person as per the Data Protection Act, 2019
Retention	The storage of information for a specified amount of time.

ACRONYMS

Acronym	Meaning
COK, 2010	Constitution of Kenya enacted in 2010
DHA, 2023	Digital Health Act enacted in 2023
DPA, 2019	Data Protection Act enacted in 2019
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officers
DQA Protocol	Kenya Health Sector Data Quality Assurance Protocol, 2014
Digital Health TWG	Digital Health, informatics and innovation TWG for Health Data Governance
HDGF	Health Data Governance Framework
HIRME ICC	Health Informatics, Research, Monitoring and Evaluation Interagency Coordinating Committee
IGAD	Intergovernmental Authority on Development
IPR	Intellectual Property Rights
IRB	Institutional Review Board
KHEA	Kenya Health Enterprise Architecture Blueprint, 2024
MoH	Ministry of Health
NHDD	National Health Data Dictionary
ODPC	Office of the Data Protection Commissioner
SAGAs	Semi-Autonomous Government Agencies
TORs	Terms of Reference
UPI	Unique Patient Identifier

FRAMEWORK OUTLINE

This Framework contains seven chapters, described below:

1	Chapter 1 provides a general introduction to the health sector in Kenya with a deeper focus on the history, status and interaction of data, information, and technology as essential interventions supporting the delivery of healthcare services.
2	Chapter 2 presents the situational analysis in Kenya articulated through the strengths, weaknesses, opportunities and threats (SWOT) approach. The aim is to highlight the current state of health data in Kenya, opportunities that abound, and, more importantly, the challenges that this policy aims to address.
3	Chapter 3 focuses on the fundamental principles of health data governance and provides an analysis of the extent of alignment between the health data governance principles and relevant local policies and legislation.
4	Chapter 4 delves deeper into providing comprehensive guidance about how health data will be governed in Kenya. This includes relevant accountability structures, roles and responsibilities across the health data ecosystem.
5	Chapter 5 describes the data management structure including the generation, processing, analysis and usage of data.
6	Chapter 6 describes the implementation plan and highlights the key activities necessary to effectively implement the Framework.
7	Chapter 7 focuses on monitoring, evaluation and learning as a method that will enable the health sector to continuously improve its investment in health data and its utilization as guided by the relevant legislation and endorsed principles.

The reader is encouraged to begin at Chapters 1 and 2 to acquire a clear understanding of the history and status of health data governance in Kenya. The contextual understanding gained from those chapters will greatly improve readability and understanding of the subsequent chapters.

1 Introduction

This chapter outlines:

1. Why Kenya needs a national health data governance framework to safeguard rights, enable equity, and guide digital transformation.
2. How health data is currently governed in Kenya and why a new approach is essential for building trust, coherence, and impact.

1.1 Overview

In recent years, Kenya has made major strides in digitising its health sector—rolling out electronic health systems, mobile applications, and data reporting platforms at an unprecedented pace. From maternal health surveillance in rural counties to smart diagnostic tools in urban centres, health data is increasingly woven into the delivery of care. Yet, this expansion has also surfaced deep structural and governance challenges. Many facilities still rely on paper records; county systems are misaligned; consent procedures vary widely; and data quality remains inconsistent. These challenges threaten not only service delivery but also public trust in the digital transformation of healthcare.

Health data refers to any information collected about an individual's health status, medical history, service interactions, or determinants of health—ranging from clinical records and insurance claims to biometric data and anonymised health statistics. When used well, it enables timely, equitable, and evidence-informed healthcare. When governed poorly, it can expose patients to risk, undermine policy decisions, or reinforce systemic inefficiencies.

Recognising its significance, Kenya has laid a strong foundation for data protection and governance:

- **The Constitution of Kenya (2010)** affirms the right to health and information, establishing the state's obligation to safeguard personal data.
- **The Data Protection Act (2019)** categorises health data as sensitive personal data and outlines lawful conditions for its processing, storage, and sharing.
- **The Health Act (2017)** mandates the Ministry of Health (MoH) to protect personal health information and promote ethical data practices.
- **The Digital Health Act (2023)** establishes the Digital Health Agency and provides a framework for interoperable, secure, and citizen-centred digital health systems.
- **The Kenya Health Policy (2014–2030)** calls for a robust, integrated, and data-informed health system grounded in principles of equity and efficiency.

These laws and policies collectively commit the Government of Kenya to build a health data ecosystem that protects rights while promoting innovation. Yet legal mandates alone are not sufficient. Fragmented systems, under-resourced data teams, and inconsistent practices at the facility and county levels hinder progress.

Why this Framework matters for every Kenyan:

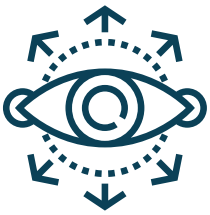
Whether it is a mother delivering a baby, a refugee seeking safety, or a senior citizen needing medication refills, safe and timely use of health data ensures their care is continuous, dignified, and effective. This Framework aims to make that a consistent reality.

This Health Data Governance Framework sets out the principles, processes, and structures that will guide how health data is protected, accessed, used, and shared in Kenya. It aligns legal mandates with operational realities, aiming to ensure that health data is governed in ways that are ethical, secure, inclusive, and impactful

1.2 Health Data Governance in Kenya

Health data governance refers to the systems, norms, and roles that determine how health data is collected, accessed, protected, used, and eventually retired. It ensures that data is treated not only as a technical asset but also as a matter of public trust, legal obligation, and social accountability.

In Kenya, the growing adoption of digital health tools, increased legal protections for personal data, and decentralisation of health governance create both opportunities and risks. Without coordination, data systems may be duplicated,



Vision:

A trusted health data ecosystem.

Mission:

To provide structure and guidance for determining, generating, processing, using, storing, retaining, sharing and sunsetting health data for purposes of optimising the inherent value of data while fostering science, echnology, and innovation in managing the health ecosystem.

misused, or underutilised. With good governance, however, data becomes a national asset that supports evidence-based decision-making and safeguards public confidence.

This Framework addresses these needs by:

- Establishing clear responsibilities among actors across the data lifecycle.
- Articulating rules and safeguards for lawful and ethical data practices.
- Promoting equity in data access and use.
- Aligning Kenya's practices with regional and global best practices.

What governance looks like in practice: A community health worker collects antenatal visit data using a mobile app; the health records officer submits this data to DHIS2; the county team validates the records; MoH aggregates national indicators; researchers request anonymised datasets for malaria forecasting; all while patient privacy is respected and security safeguards are in place.

The Framework applies across the data lifecycle:

- Data generation and collection
- Access and sharing protocols
- Anonymisation, pseudonymisation, and consent management
- Analysis and visualisation
- Storage, retention, archiving, and secure disposal

Governance failures—such as unclear consent, unauthorised sharing, or inaccurate data reporting—can undermine public trust, legal compliance, and care continuity. Conversely, strong governance promotes resilience, accountability, and progress.

Key Objectives of the Framework

1. **Inclusive Participation:** Involve diverse stakeholders—including government, counties, civil society, academia, and communities—in defining data needs and governance models.
2. **Transparency and Privacy:** Promote informed consent, robust data stewardship, and

accountability mechanisms to protect privacy.

3. **Coordination and Partnership:** Foster collaboration among public, private, and cross-sectoral actors through shared governance platforms.
4. **Trust and Accountability:** Build confidence in digital systems through clear oversight, redress mechanisms, and performance monitoring.
5. **Capacity Strengthening:** Develop skills, tools, and systems at all levels to support consistent and lawful data use.

1.3 Scope

This Framework applies to all health data generated, processed, or shared within Kenya's health sector—whether by public institutions, private facilities, non-governmental actors, or academic partners. It is relevant to data in all formats: paper-based, hybrid, or fully digital.

It also provides guidance for:

- Cross-border data sharing involving Kenya and other states or regional bodies.
- Use of health data in research, planning, service delivery, and policy development.
- Alignment of sector-wide data practices with the Data Protection Act, 2019, and the Digital Health Act, 2023.

Out of Scope:

This Framework does not apply to health or wellness data generated solely for personal use and stored exclusively on individual-owned devices or platforms—unless integrated with formal health systems (e.g. national EMRs or county dashboards).

Categories of Health Data

1.3.1 Administrative Data

Institutional data related to health operations, such as facility registration, staff rosters, payroll, and procurement records. Managed primarily by health facility administrators and county-level HRH officers.

1.3.2 Aggregate Health Data

Summarised, de-identified data used for monitoring and evaluation, public reporting, and planning. Derived from facility reports, surveys, and information systems like KHIS.

1.3.3 Individual-Level Health Data

Personal health records collected through service delivery, community outreach, or surveys. May be identifiable (e.g. with names or ID numbers) or anonymised. Includes:

- Medical records and encounter data
- Diagnostic and laboratory results
- Referral and claims information
- HRH tracking and supervision reports

1.3.4 Digital Exhaust Data

Secondary data generated from user interactions with digital platforms—e.g. timestamps, audit trails, device performance logs, and metadata from eHealth tools. May include sensitive information if linked to individuals.

1.3.5 Research for Health Data

Data collected under formal research protocols, either as primary studies or through the secondary use of routine health data. Governed by ethical review and institutional access protocols.

Who interacts with what data?

Data officers manage administrative and individual-level records; researchers use aggregate and research data; regulators monitor digital exhaust; and MoH uses all types for national policy and planning.

Together, these categories reflect the diversity and complexity of Kenya's health data ecosystem. Governance provisions must therefore be equally robust, adaptive, and inclusive.

1.4 Intended Audience

This Framework is designed to guide a broad spectrum of stakeholders involved in the generation, use, governance, and protection of health data in Kenya. Recognising the complexity and interconnectedness of the health system, it intentionally speaks to both individual professionals and institutional actors whose roles and responsibilities influence the health data lifecycle.

Individual stakeholders include:

- Healthcare workers at all levels, from community health volunteers to specialists in tertiary facilities
- Health records and information officers, tasked with data entry, quality assurance, and reporting
- ICT personnel responsible for system administration, maintenance, and security
- Data analysts and planners who interpret data to guide resource allocation and service delivery
- Researchers and academic professionals who generate evidence through primary and secondary data analysis
- Policymakers and programme managers at national and county levels who rely on health data for strategy and oversight

Institutional stakeholders encompass:

- National government agencies, led by the Ministry of Health, as stewards of policy and standards
- County governments and departments of health as key implementers and custodians of service delivery data
- Public and private health facilities, whose day-to-day operations generate vast volumes of health data
- Faith-based and non-governmental organisations providing health services or health advocacy
- Civil society organisations that represent patient and community interests in matters of data justice and ethics
- Academic and research institutions undertaking data-driven studies to inform policy and innovation
- Health insurance providers and financing institutions whose processes rely on accurate and protected health information
- Technology providers and vendors responsible for the development and maintenance of digital health solutions

These stakeholders can be grouped into three key clusters: frontline actors who generate and manage data (e.g. health workers, records officers); system stewards who set policy and provide oversight (e.g. MoH, counties); and data intermediaries who analyse, secure, or interpret data (e.g. researchers, ICT officers, developers).

While many of these entities operate at different levels of the system, this Framework aims to foster a shared understanding of standards, responsibilities, and ethical expectations. It recognises that effective governance requires aligned effort across the ecosystem.

Importantly, the Framework also affirms the centrality of data subjects—the individuals whose information is collected and managed. While not implementers, their rights and expectations underpin the spirit and letter of this Framework. The Data Protection Act, 2019 and the Digital Health Act, 2023 mandate that such individuals have rights to informed consent, access, correction, and protection from misuse. As such, all other stakeholders have a duty to uphold these rights in practice.

vThe Framework aims to build shared accountability across this diverse landscape, enabling health data to serve the public good while protecting individual rights.

1.5 Exclusions

This Framework is primarily concerned with the governance of health data that is part of the formal health system in Kenya. It applies to all public, private, and civil society actors who generate, process, share, or use health data while delivering health services, managing health systems, or conducting health-related research. It is also applicable to data in any format—whether paper-based, hybrid, or fully digital.

However, not all forms of health-related data fall within the scope of this Framework. Specifically, it excludes:

- **Personal health and wellness data** that is self-generated and used exclusively by individuals for their own purposes (e.g., logs from mobile fitness applications, home-based blood pressure monitors, or digital journaling tools).
- **Data that is not shared, processed, or integrated** into a formal health information system, service, or research activity.

In practice, this means that an individual tracking their step count on a smartwatch is outside the governance domain of this Framework—**unless** that data is submitted to a health provider, facility, digital platform, insurer, or government body. Once shared with a health actor or integrated into a health system, such data becomes subject to the governance requirements outlined in this document, including relevant safeguards under the DPA, 2019 and DHA, 2023.

This distinction is important to prevent regulatory overreach while maintaining a clear line of accountability when data enters the formal health domain. It also reflects the need to respect personal autonomy while enforcing protections where health data is used in public or institutional settings.
By contrast, any data shared with, accessed by, or processed through formal health systems—regardless of its origin—is governed under this Framework.

1.6 Rationale

Kenya's digital transformation agenda has catalysed significant innovation and investment in health information systems. From digital logistics management to electronic medical records, data dashboards, and patient monitoring platforms, digital tools are increasingly embedded across the continuum of health service delivery.

Despite these advances, there remains an urgent need to consolidate and harmonise the governance of health data across the country. Stakeholder consultations, document reviews, and technical analyses have revealed persistent issues that undermine the value, integrity, and protection of health data in Kenya. These include:

Fragmentation and Duplication: Multiple platforms and actors collect data using different standards and tools. For instance, facilities may use parallel systems—some partner-funded, others government-deployed—without common interoperability. This results in duplication, inconsistencies, and user fatigue.

Policy Misalignment: Organisations often have their own policies on data collection, sharing, and retention, but these may not align with national laws such as the DPA or be consistent across counties. Programme-specific rules (e.g., for HIV data) may not apply to broader health information systems.

Unclear Roles and Responsibilities: In many settings, especially at county and facility levels, the question of "who owns what data and who decides what happens to it" remains unresolved. This leads to gaps

in accountability and limited enforcement of privacy safeguards.

Limited Data Use: While much effort is invested in collecting data, its use for decision-making remains low. Access is often restricted, systems are not user-friendly, or data quality issues prevent meaningful analysis.

> **Example:** In one county, maternal health data is split across three systems: one hosted by the county government, one by an international partner, and one managed by the national referral system. The systems do not speak to each other (not integrated). Consent procedures differ. Reporting timelines are not synchronised. The result is delayed decision making, staff burnout, and incomplete policy evaluation and incorrect reporting.

These challenges point to the absence of a shared, enforceable, and rights-based framework that defines what good health data governance looks like. The absence of a framework risks do not only lead to inefficiency but also legal breaches, data misuse, and erosion of public trust.

This document responds to that need by providing a common reference point—grounded in law, aligned with practice, and designed to grow with the system. It seeks to:

- Ensure clarity of roles and responsibilities across data lifecycle actors
- Encourage consistency across data governance processes nationwide
- Promote ethical and lawful handling of sensitive health data
- Enable value creation from health data, including for service improvement, planning, research, and innovation

It is also responsive to Kenya's commitments under the Digital Health Act and the DPA, as well as the African Union's call for harmonised digital health governance across Member States. By laying out a coherent national approach, this Framework enables Kenya to lead by example in digital trust and accountability in the health sector. This Framework translates legal mandates into operational clarity, aligning everyday practices with national values and global norms.

1.7 Framework Development Approach

This Framework is the product of an inclusive and technically rigorous development process, undertaken to ensure legitimacy, relevance, and practicality. From inception to validation, the approach reflected Kenya's longstanding commitment to participatory governance and cross-sector collaboration as shown in Figure 1 and 2.

Under the leadership of the Ministry of Health, the Framework was developed through a combination of:

- In-person and virtual stakeholder consultations
- Iterative co-writing and review workshops
- Legal and policy alignment with the DPA (2019), DHA (2023), and global data governance principles

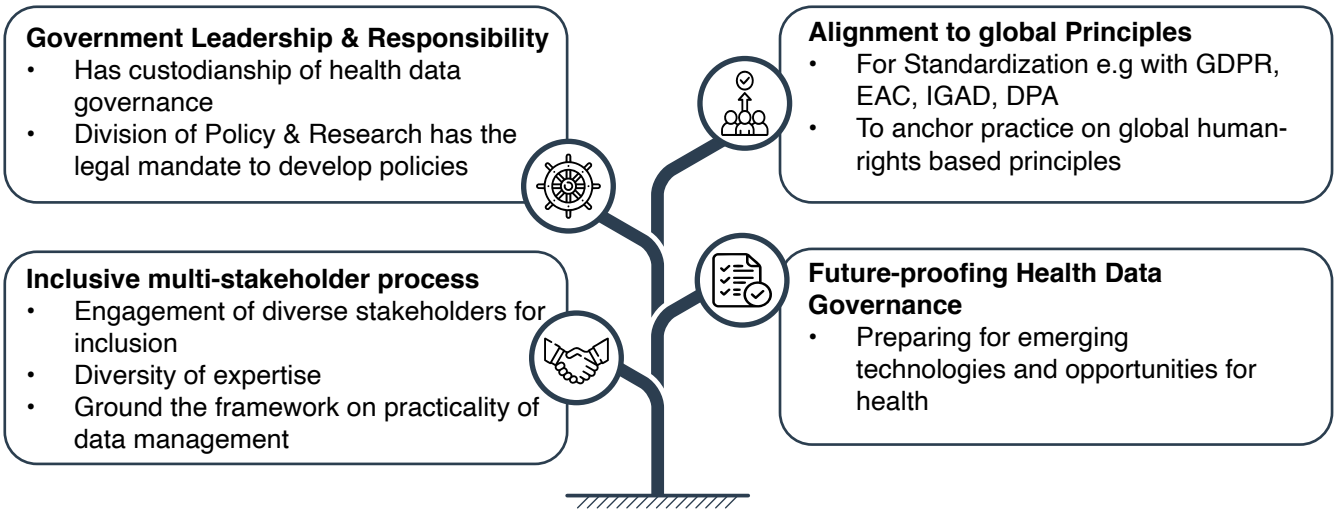


Figure 1: Approach to Framework Development

The process unfolded through the following milestones:

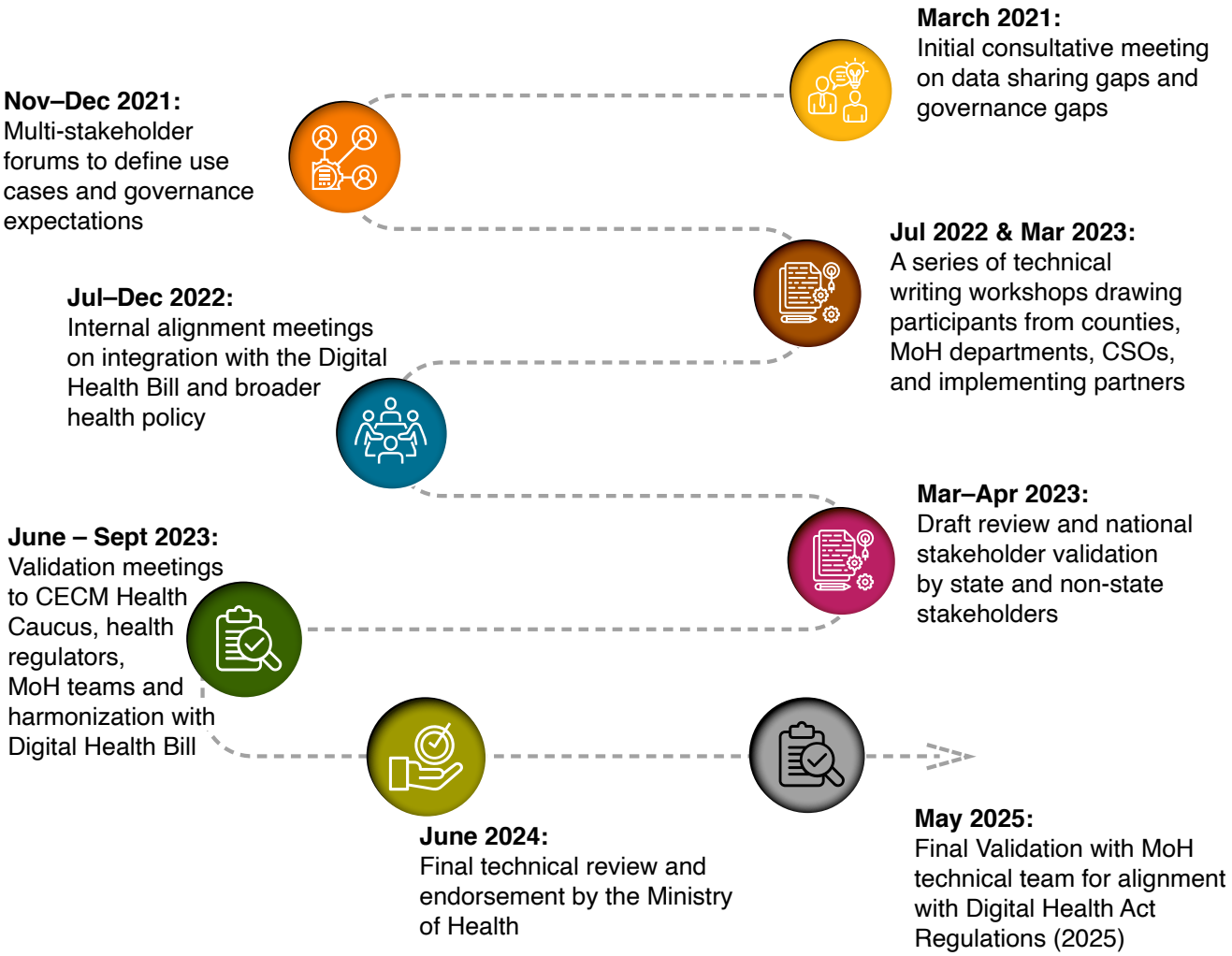


Figure 2: Inclusive Development Process: Timeline of Events.

The process was grounded in the recognition that data governance is both technical and political—requiring legal clarity, institutional ownership, and social legitimacy. Special care was taken to ensure that the voices of counties, implementers, data managers, and affected communities were reflected.

The final Framework is not a static document. It is designed to evolve in step with new technologies, data uses, legal interpretations, and lessons from implementation. As such, it will be reviewed every 3–5 years or as required to remain fit-for-purpose in a rapidly changing health data landscape. The Ministry of Health encourages continued engagement from all stakeholders as implementation progresses and lessons emerge.

1.8 Summary

Chapter 1 of this Framework introduces the critical need for a comprehensive health data governance system in Kenya. It highlights the rapid digital transformation of Kenya's health sector and the increasing reliance on health data for decision-making, service delivery, and public health. However, it also identifies significant challenges, including fragmented systems, inconsistent data quality, and insufficient data privacy protections, which undermine the potential benefits of health data.

This chapter emphasizes that a robust governance framework is essential to safeguard individual rights, ensure equitable access to health data, and promote transparency and trust in digital health systems. By aligning with Kenya's constitutional, legal, and policy frameworks—such as the Constitution of Kenya (2010), Data Protection Act (2019), and Digital Health Act (2023)—the Health Data Governance Framework (HDGF) is positioned as the solution to address these challenges. The chapter also outlines the foundational principles, processes, and structures that will guide health data governance in Kenya.

Chapter 2 delves deeper into the current state of health data governance in Kenya, examining the legal, policy, and technical landscape. It identifies key gaps, risks, and opportunities that underscore the necessity for a more cohesive, future-ready governance approach. This analysis sets the stage for the comprehensive solution the HDGF offers, ensuring it aligns with the evolving needs of Kenya's health data ecosystem.

2 Situational Analysis

This chapter outlines:

1. How Kenya's health data governance landscape has evolved and the policy, legal, and technical milestones that shaped it.
2. Why key gaps, risks, and opportunities now demand a more coherent, future-ready approach to governing health data.

2.1 Introduction

Over the past decade, Kenya's health sector has experienced a transformative shift in how health data is collected, stored, processed, and used. Traditionally dominated by manual, paper-based systems, the sector has rapidly transitioned to digital platforms, integrating mobile applications, electronic medical records (EMRs), health information exchanges, and facility dashboards. These advancements have enabled the generation of real-time, high-quality health data that supports faster decision-making, improved service delivery, and stronger program performance.

Health data—whether derived from individual patient interactions, facility reports, or aggregated program monitoring—is now recognised as a strategic national asset. The Data Protection Act (2019) affirms this, classifying health data as sensitive personal data deserving of the highest standards of protection. When effectively governed, health data can optimise planning, reduce costs, and deliver timely insights. Yet, when mismanaged, it can erode public trust, expose individuals to harm, and hinder the continuity and quality of care.

Kenya's digital maturity in health, while promising, remains uneven. Many counties still operate in hybrid environments where digital tools coexist with paper registers. Interoperability gaps persist across partner-driven systems, national platforms, and county applications. Consent procedures vary widely, and there is no uniform understanding of who owns data or how it should be used and shared. This fragmentation exposes the sector to risks of inefficiency, privacy breaches, and inconsistent application of legal safeguards.

To address these challenges and realise the full value of health data, the Ministry of Health, guided by the Kenya Health Sector Partnership and Coordination Framework (2018–2030), led the development of this national Health Data Governance Framework. The process was anchored in the recognition that good governance is not just a technical function—it is a matter of public interest and institutional legitimacy.

The evolution of Kenya's health data governance ecosystem is reflected in a growing body of legislation, policies, and technical guidelines. These instruments—spanning from the Constitution of Kenya to the Digital Health Act of 2023—have progressively expanded the scope, enforcement mechanisms, and institutional arrangements governing health data. Figure 3 illustrates this trajectory, highlighting key milestones that form the legal and strategic foundation of this Framework.

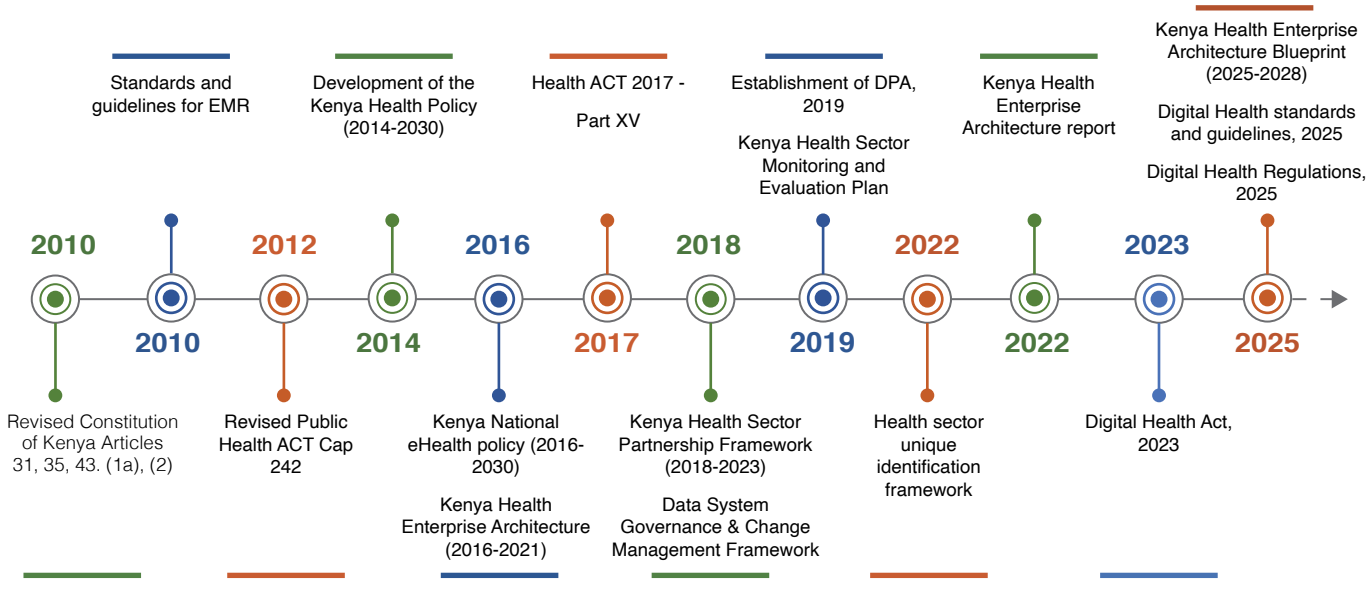


Figure 3: Development Timeline of Governance Legislation and Policy Documents in Kenya.

This Framework builds on a robust legal and policy foundation, including the Constitution of Kenya (2010), the Health Act (2017), the Data Protection Act (2019), and the Digital Health Act (2023). It seeks to translate these legal commitments into actionable guidance on how data should be collected, shared, protected, and used within Kenya's health system—whether at the national referral hospital, a county maternity ward, or a community outreach program.

Through a systematic review of legislation, stakeholder consultations, and technical assessments, the Ministry and its partners have mapped the current state of data governance. This includes identifying what is working, where gaps exist, and which risks and opportunities lie ahead. The resulting Framework offers not only a diagnosis of the current landscape but a shared vision for responsible, secure, and equitable health data governance that adapts to a rapidly evolving digital health environment.

2.2 The Regulatory Landscape

Kenya's approach to health data governance is underpinned by a comprehensive and evolving legal framework. This framework is shaped by constitutional rights, statutory obligations, and sector-specific policies that collectively safeguard privacy, promote access to information, and foster ethical data use.

At the core of this regulatory landscape is the recognition that health data is not just a technical resource—it is intrinsically linked to the rights, dignity, and welfare of individuals. The laws outlined below provide the foundation upon which the Health Data Governance Framework is built.

2.2.1 Constitution of Kenya, 2010

The Constitution is the supreme law of the land and provides key principles that frame the governance of health data:

- **Article 31 (c) and (d):** Protects every individual's right to privacy, including protection from unnecessary disclosure of personal and family information and from the infringement of communications.
- **Article 35:** Guarantees every citizen the right to access information held by the state or other parties when required for the exercise or protection of a right.
- **Article 43 (1)(a):** Affirms the right of every person to the highest attainable standard of health.
- **Article 43 (2):** Mandates access to emergency medical treatment as a right.

These provisions place a constitutional obligation on the state and all health actors to safeguard personal health data, ensuring it is handled with integrity, confidentiality, and respect for individual autonomy.

2.2.2 The Health Act, 2017

The Health Act aims to establish a unified health system that aligns the roles of national and county governments. It defines the architecture for coordinated service delivery, regulation of health professionals, and the provision of health products and technologies.

- Part XV of the Act recognises digital health (eHealth) as a legitimate mode of service delivery.
- It mandates the Ministry of Health to establish and maintain a comprehensive, integrated health information system, reinforcing the need for structured governance of health data across the health ecosystem.

2.2.3 The Digital Health Act, 2023

Enacted as part of the broader Universal Health Coverage (UHC) reforms, the Digital Health Act provides the most explicit legal grounding for health data governance in Kenya:

- **Part II** establishes the **Digital Health Agency** and designates it as the official **Health Data Custodian.**

- **Section 15(1)** establishes the **Comprehensive Integrated Health Information System (CIHIS)**.
- **Parts IV and V** outline the principles, classifications, and protections related to **Health Data Governance**, including obligations around confidentiality, privacy, and security.
- **Section 43** defines how data should be managed in the provision of eHealth services.
- **Section 47** regulates the sharing of personal health data outside Kenya for specific purposes, such as **Health Tourism**.

This Act aligns data governance with service delivery reforms, ensuring that digital health investments are matched with legal protections.

2.2.4 Data Protection Act, 2019 (DPA)

The DPA is Kenya's principal legislation on data privacy. It provides cross-cutting provisions that apply to all forms of personal data, with special emphasis on **sensitive personal data** such as health records:

- It defines roles for **Data Controllers** and **Data Processors**, and places accountability on them to protect individual rights.
- The Act requires lawful, fair, and transparent data processing, and mandates informed consent as a precondition for handling health data.
- It provides for data portability, access, correction, and the right to object to processing—making it one of the most progressive privacy laws in Africa.

The DPA is directly applicable to all health sector actors, including government institutions, private facilities, NGOs, and researchers

2.2.5 Complementary Legislation

Several other Acts complement the constitutional and health sector-specific laws by addressing broader aspects of data use, communications, and cybersecurity:

- **Public Health Act, 2012:** Focuses on public health protection but lacks explicit provisions on digital data governance.
- **Kenya Information and Communications Act, 2011:** Recognises electronic records as legal documents and provides standards for their retention.
- **Access to Information Act, 2016:** Empowers citizens to request and receive public information and obligates government entities to disclose relevant data.
- **Computer Misuse and Cybercrimes Act, 2018:** Provides legal safeguards for the confidentiality, integrity, and availability of data systems and promotes secure information infrastructure.

Together, these laws ensure that the management of health data in Kenya is not only legally compliant but also responsive to the realities of digital transformation.

2.2.6 Sector Policies and Frameworks

The In addition to legislation, Kenya has developed a rich portfolio of health sector policies and implementation frameworks that shape health data governance:

- **Kenya Health Policy (2014–2030) and Kenya National eHealth Policy (2016–2030):** Promote data-driven decision-making and ethical data use.
- **Data Quality Assurance (DQA) Protocol (2014):** Establishes methodologies for routine data validation and quality improvement.
- **Standards and Guidelines for Electronic Medical Records (2017):** Sets minimum technical and functional standards for EMRs.
- **Data, System Governance and Change Management Framework (2018):** Defines roles, processes, and standards for effective information system governance.
- **Monitoring and Evaluation Plan (2019):** Outlines national approaches to data-driven performance monitoring.

- **Kenya Health Sector Partnership and Coordination Framework (2018–2030):** Facilitates multi-stakeholder collaboration on data and service delivery.
- **Health Sector Unique Identification Framework (2022):** Introduces the **Unique Patient Identifier (UPI)** for enhanced health clients identification and service continuity..
- **Standards and Guidelines for Electronic Medical Records (2017):** Sets minimum technical and functional standards for EMRs.
- **Kenya Health Enterprise Architecture (2025):** Establishes the digital backbone for integrated, secure, and interoperable health information systems. The Kenya Health Enterprise Architecture (KHEA) provides a holistic blueprint for organizing digital health systems and services, with governance as a cross-cutting enabler. It illustrates how different health information components—including data services, infrastructure, interoperability layers, and governance roles—interact within an enterprise model. Figure 4 below summarizes this architecture, showing how health data governance fits within Kenya's digital health ecosystem.

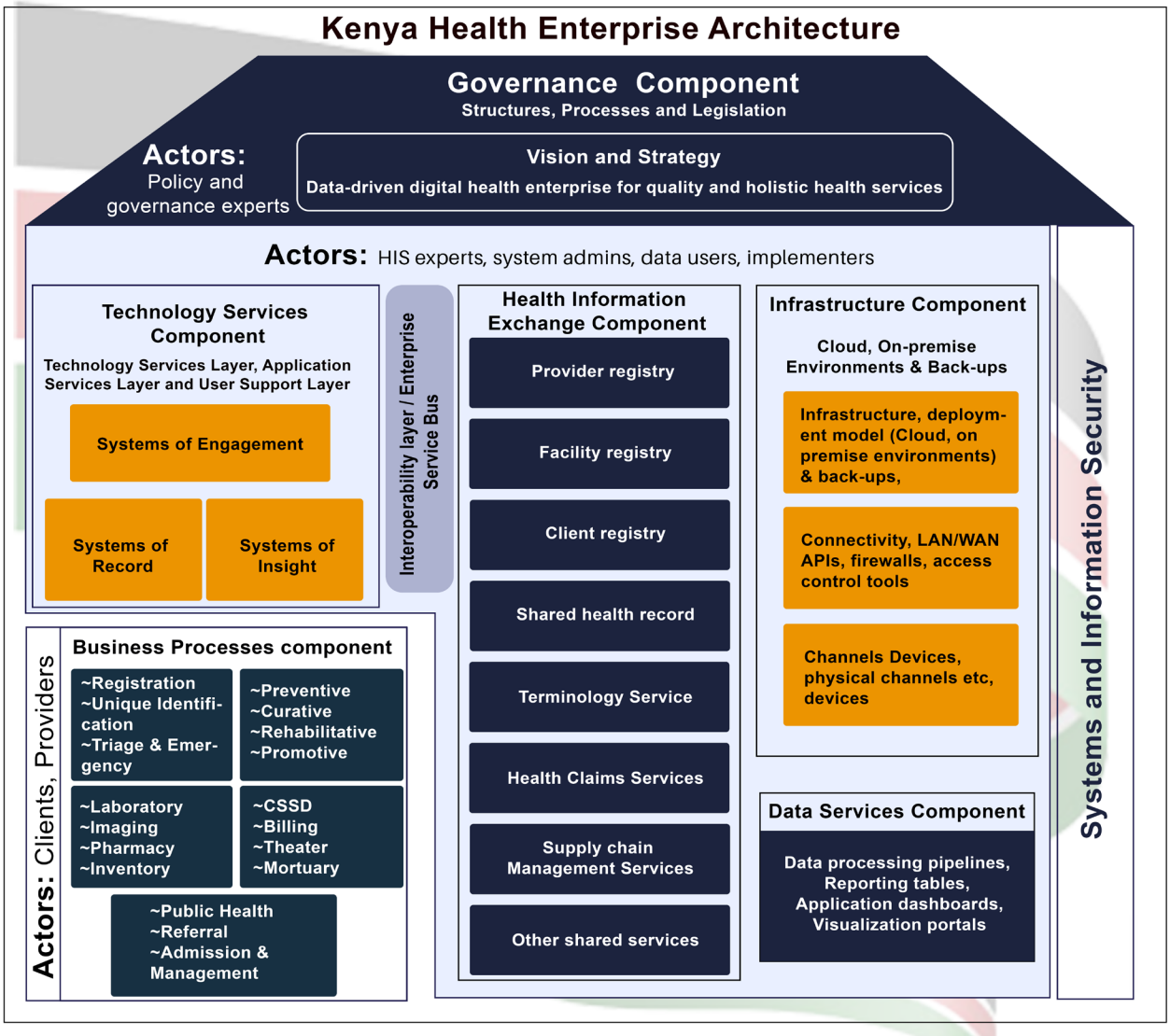


Figure 4: Kenya Health Enterprise Architecture (KHEA)

Each of these instruments adds practical specificity to Kenya's vision of responsible, people-centred, and resilient digital health systems.

What this means for health data governance:

The regulatory landscape provides a strong foundation but coordination, operational clarity, and continuous capacity strengthening are essential. This Framework leverages existing laws to offer a unified, actionable approach to governing health data across sectors and systems.

Kenya's health data management landscape has evolved significantly over the past decade, with growing stakeholder alignment around standardized governance practices. Legislative milestones—such as the Data Protection Act (2019) and the Digital Health Act (2023)—have laid a solid foundation, anchored by the designation of the Digital Health Agency as the health data custodian. Despite this progress, gaps remain; rapid technological change continues to outpace policy implementation; technology adoption is uneven; and cybersecurity risks persist. Meanwhile, underinvestment, workforce limitations, and shifting sectoral priorities threaten the sustainability of data governance gains. To address these challenges, strategic investments are needed—in capacity building, policy alignment, digital infrastructure, and security safeguards—to ensure Kenya fully realizes the value of health data while protecting the rights of its citizens.

2.3 Informed Insights

The development of this Health Data Governance Framework was informed by both a review of existing legal and policy instruments and a set of structured consultations with key stakeholders. This dual approach ensured that the Framework is not only aligned with Kenya's legal obligations and sectoral policies, but also responsive to real-world practices, challenges, and opportunities observed within the country's evolving health data ecosystem.

To establish an accurate baseline, the Ministry of Health (MoH) and its stakeholders undertook a semi-formal information-gathering process involving representatives from a wide array of actors, including other government ministries and agencies, county governments, development partners, professional health associations, the private sector, academic institutions, and research organisations. Information was gathered through a combination of online and face-to-face key informant interviews and focus group discussions.

2.3.1. Evolving Policy and Legal Environment

Stakeholders consistently acknowledged that Kenya has a mature and rapidly evolving legal and policy environment for data governance. There was broad consensus that the Data Protection Act (2019), the Digital Health Act (2023), and other supporting regulations offer a robust foundation for protecting and managing health data. The legislative architecture was viewed as adequate in principle, but stakeholders noted the need for better operational clarity and consistency in interpretation, especially across counties and implementing partners.

Participants noted the importance of ensuring alignment in the application of different legislative instruments, such as the DPA (2019) and the Access to Information Act (2016). While personal data protection is well-articulated in the DPA, stakeholders observed a lack of guidance on how aggregated, anonymised, or de-identified health data should be governed—particularly in contexts involving secondary use or cross-border sharing.

2.3.2. Heterogeneity in Information System Models

The consultations revealed that Kenya's health information systems remain highly heterogeneous. Stakeholders described the coexistence of multiple system models in active use ranging from fully manual, paper-based systems to hybrid paper-digital platforms, and fully digitalised environments. This diversity reflects Kenya's decentralized governance structure, as well as varying levels of investment and digital maturity across counties and institutions.

This heterogeneity was acknowledged as both a challenge and an opportunity. While it complicates standardisation, it also presents a unique chance to test and scale the governance model proposed in this Framework in diverse settings, potentially generating valuable insights for future refinement and cross-country learning.

2.3.3. Emerging Demand for Digital Innovation

Informants also highlighted the growing recognition of data as a strategic asset, particularly when considering emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), Deep Learning, and the Internet of Things (IoT). Many organisations expressed commitment to investing in these technologies for health surveillance, diagnostics, predictive analytics, and resource optimisation. There was agreement that data governance must evolve alongside these innovations to address both new opportunities and associated risks.

2.3.4. Governance Capacity and Institutional Readiness

Despite the enabling policy environment, stakeholders noted that general governance of data has not fully matured within government institutions. In many settings, data protection policies are not yet institutionalised, and capacity gaps persist at both technical and leadership levels. These gaps were cited as barriers to the implementation of data governance practices, including those related to consent, data sharing, and risk management.

Participants recommended strengthened collaboration between the Ministry of Health and the Office of the Data Protection Commissioner (ODPC) to accelerate capacity building, streamline compliance, and improve policy harmonisation across public and private health sector actors.

2.3.5. Opportunities to Build Public Trust and Resilience

The stakeholder insights also pointed to an emerging opportunity for Kenya to model progressive health data governance by increasing awareness, promoting understanding, and building capacity across all levels of the health sector. Stakeholders recognised that consistent adherence to the principles enshrined in the DPA, 2019—when appropriately contextualised to the realities of health service delivery—could enhance both operational efficiency and public trust

.

At the same time, there was consensus that rising investments in digital health infrastructure and systems have also elevated risks, including those associated with data breaches and cybercrime. These risks, if left unaddressed, could undermine confidence in health data systems and compromise the sector's ability to fully realise the value of its data assets.

2.3.6. Implications for the Framework

The cumulative insights from this stakeholder engagement process underscore the need for a practical, context-sensitive, and legally grounded health data governance framework that can:

- Translate legislative provisions into operational policies and procedures.
- Offer clear and consistent guidance for the

governance of both identifiable and non-identifiable health data.
- Promote institutional alignment and capacity development across public and private actors.
- Safeguard individual rights while enabling safe and ethical data innovation.

The Framework, as set forth in the following chapters, is designed to respond to these needs while reinforcing Kenya's leadership in shaping inclusive, resilient, and rights-based digital health systems.

2.4. Summary

Chapter 2 provides a comprehensive Situational Analysis of Kenya's health data governance landscape. It traces the evolution of health data management in the country, highlighting the significant strides made in digitising health systems and the integration of electronic health records, mobile applications, and data platforms. Despite these advancements, the chapter identifies several gaps and challenges, such as fragmented data systems, lack of interoperability, varying consent practices, and inconsistent data quality, which hinder the effectiveness of the health data ecosystem.

The chapter also underscores the need for a cohesive governance framework that can address these issues and promote better data management, privacy, and security across the health sector. It outlines Kenya's existing legal and regulatory landscape, including key legislation such as the Constitution of Kenya (2010), Health Act (2017), and Data Protection Act (2019), which collectively lay the groundwork for a more structured approach to health data governance. However, the analysis reveals that these laws and policies are not yet fully operationalised or harmonised across the country's decentralized health system.

In **Chapter 3**, the focus will shift to the Global Health Data Governance Principles and their contextualisation for Kenya. These principles, which form the ethical backbone of the Health Data Governance Framework (HDGF), will be examined within the context of Kenya's legal and institutional landscape. The chapter will outline how global best practices can be adapted to local needs, ensuring that Kenya's health data governance system is both internationally compliant and locally relevant.

3 Principles for Health Data Governance

This chapter outlines:

1. The global principles for health data governance and their relevance to Kenya.
2. How the principles were adapted to align with Kenya's legal and policy context.
3. The three core objectives that guide their application: protecting people, promoting the value of health data, and prioritising equity

3.1 Introduction

In Kenya's rapidly evolving digital health landscape, principles serve as both ethical anchors and practical guides. They articulate the values that should inform decisions at every stage of the health data lifecycle especially where technology, regulation, and human rights intersect.

Health data governance principles define not only what is legal but also what is just, fair, and responsive to the lived realities of individuals and communities. They confront foundational questions: Why do we collect health data? Who decides how it is used? Who is protected and who may be excluded or harmed if governance is weak or inconsistent?

To navigate these questions, Kenya has adopted and contextualised the Global Principles for Health Data Governance, as advanced by the World Health Organization and other normative bodies. These principles were carefully reviewed, tested against national laws, and validated through multi-stakeholder consultations, ensuring alignment with the Constitution (2010), Data Protection Act (2019), Digital Health Act (2023), and Kenya's broader obligations under Universal Health Coverage (UHC).

The outcome is a uniquely Kenyan articulation of health data governance principles—anchored in Kenya's legal frameworks, informed by policy experience, and responsive to local realities. Rather than presenting a static list of principles, the Framework clusters them around three interconnected governance objectives, each guiding a set of more specific, enforceable commitments. As illustrated in Figures **5a and 5b,** these objectives are presented in both English and Kiswahili, affirming commitment to cultural relevance and accessibility in health data governance:

- **Kulinda Watu** (Protecting People)
- **Kukuza Thamani ya Takwimu za Afya** (Promoting the Value of Health Data)
- **Kutanguliza Usawa** (Prioritising Equity)

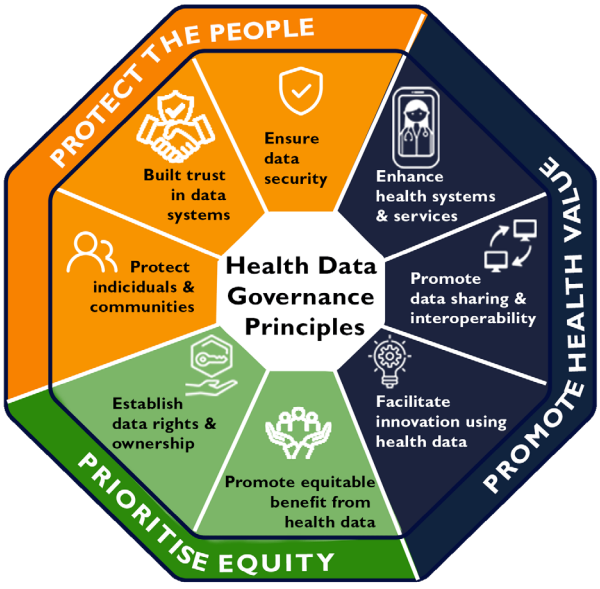
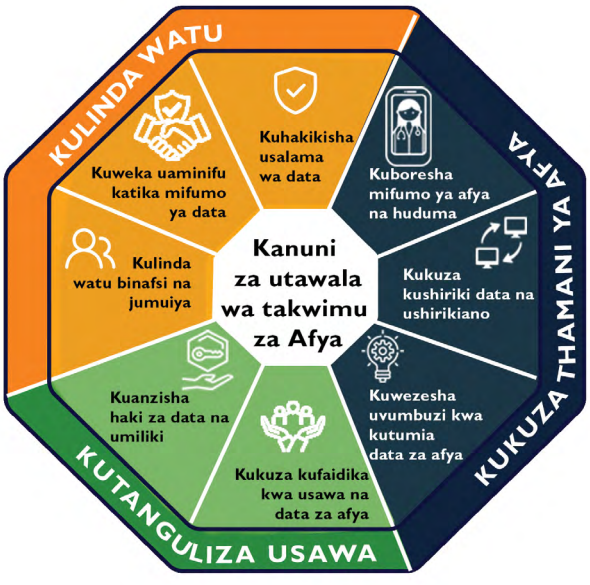


Figure 5a: Principles of health data governance.



Kielelezo 5b: Kanuni za usimamizi wa data za afya.

Each objective represents a core goal of health data governance in Kenya. Within each cluster, a set of specific principles defines how the objective will be realised —through lawful processing, inclusive design, equitable benefit-sharing, secure systems, and data-driven innovation.

This chapter introduces each objective, and the principles nested within it, detailing their legal foundation, normative logic, and operational implications for Kenya's health system.

3.2 Foundation and Legal Compatibility of the Principles

The health data governance principles adopted in this Framework are rooted in international best practice but have been deliberately localised to fit Kenya's legal and institutional landscape. The process of adapting the global principles involved a legal, normative, and practical review to determine their compatibility with Kenyan law and policy priorities. This ensured that the principles are not only aspirational but also lawful, enforceable, and relevant to the governance of health data in Kenya.

This legal review confirmed that each of the three principles aligns with and reinforces provisions in the following national instruments:

- The Constitution of Kenya (2010) – Article 31 guarantees the right to privacy, while Article 43 affirms the right to the highest attainable standard of health.
- The Data Protection Act (2019) – Outlines data protection principles, defines sensitive personal data (including health data), and sets conditions for lawful processing.
- The Health Act (2017) – Emphasises patient confidentiality and the protection of personal health information as part of ethical service delivery.
- The Digital Health Act (2023) – Establishes the Digital Health Agency as the custodian of health data and mandates the creation of a health data governance framework based on rights, equity, and security.

In addition to statutory instruments, the Data Systems Governance and Change Management Framework (2018) served as a foundational reference in shaping how principles would be interpreted and applied across Kenya's decentralised health system. That framework already acknowledged the need for a principled approach to defining roles, decision rights, and accountability mechanisms within the digital transformation of health.

Furthermore, Kenya's endorsement of the Universal Health Coverage (UHC) agenda and participation in regional digital health initiatives underscores the importance of values such as equity, security, and data-driven innovation—values that are embedded in the principles outlined here.

Through this rigorous alignment process, it was affirmed that the principles of protecting people (kulinda watu), promoting the value of health data (kukuza thamani ya takwimu za afya), and prioritising equity (kutanguliza usawa) not only reflect international consensus but also strengthen Kenya's existing legal and ethical commitments. They provide an ethical lens through which to interpret and operationalise Kenya's evolving digital health governance landscape.

As such, these principles offer a common reference point for actors across the health data ecosystem—enabling shared understanding and harmonised application of laws, policies, and safeguards that protect individual rights while promoting system-wide accountability and innovation.

3.2.1 Governance Objective 1: Protecting People (Kulinda Watu)

Safeguard Human Dignity, Rights, and Security in the Use of Health Data

3.2.1.1 Objective Overview

The first and most foundational governance objective is to protect people—kulinda watu. This means safeguarding individuals, groups, and communities in Kenya from harm, exploitation, discrimination, or exclusion arising from the misuse or mismanagement of health data.

The increasing digitisation of Kenya's health system introduces powerful capabilities—but also new vulnerabilities. As health data flows through mobile platforms, cloud storage, electronic health records, and cross-border systems, the risks of privacy breaches, misuse, or surveillance intensify. These risks are not theoretical; they directly affect public trust, willingness to participate, and the overall legitimacy of health programmes.

Kulinda Watu asserts that health data governance must not only comply with legal thresholds—it must actively promote ethical data practices that respect individual rights, protect community agency, and build trust across the health ecosystem.

3.2.1.2 Clustered Principles Under this Objective

To achieve this objective, the following core principles are upheld:

Principle 1: Protect Individuals and Communities (Kulinda watu binafsi na jamii)

Health data systems must avoid profiling, exploitation, or discrimination. Governance must prioritise dignity, autonomy, and agency for all data subjects—particularly vulnerable or marginalised populations.

Principle 2: Ensure Data Security (Kuhakikisha usalama wa data)

Technical and organisational safeguards must be applied across all stages of the data lifecycle—collection, storage, sharing, and disposal. This includes encryption, secure infrastructure, role-based access controls, and continuous system monitoring.

Principle 3: Build Trust in Data Systems (Kuweka uaminifu katika mifumo ya data)

Trust must be built through transparency, consent, user feedback, and continuous community engagement. Mechanisms should exist for audit trails, complaints, and redress—grounded in legal rights and ethical norms.

3.2.1.3 Systemic Impact

By enshrining these principles under Kulinda Watu, Kenya affirms that health data governance is a human rights matter not simply a technical or administrative concern. It creates a foundation of trust that underpins all other objectives, including data sharing, innovation, and equitable benefits.

Protecting people means ensuring that Kenya's digital health transformation is inclusive, safe, and grounded in both constitutional rights and community realities.

3.2.2 Governance Objective 2: Promoting the Value of Health Data (Kukuza Thamani ya Takwimu za Afya)

Maximise the Benefit of Health Data Through Responsible Use, Innovation, and System Strengthening

3.2.2.1 Objective Overview

Health data is a national asset. When effectively governed, it powers better decisions, stronger systems, and improved health outcomes. The second objective of this Framework—Kukuza Thamani ya Takwimu za Afya—calls on all health actors to unlock the full value of data in a way that is ethical, equitable, and beneficial to all.

Promoting the value of health data is not about monetization, it is about **enhancing utility.** It means turning data into actionable insights,

enabling timely interventions, and driving innovations that solve real-world problems.

This objective affirms that data must be used—not hoarded—and that value must be created for all stakeholders, especially patients and frontline providers.

3.2.2.2 Clustered Principles Under this Objective

The principles under this objective focus on strengthening health systems, improving data flow, and enabling innovation:

Principle 1: Enhance Health Systems and Services (Kuboresha mifumo ya afya na huduma)

Data must drive continuous system improvement at all levels. From planning to policymaking, data should support responsiveness, resilience, and results across Kenya's health sector.

Principle 2: Promote Data Sharing and Interoperability (Kukuza ushirikiani wa data na ushirikiano)

Systems must "talk/communicate" to one another. Data should flow securely and seamlessly across platforms, institutions, and levels of care, enabling a single patient journey and a unified view of population health.

Principle 3: Facilitate Innovation Using Health Data (Kuwezesha uvumbuzi kwa kutumia data za afya)

Health data should power responsible innovation. Whether through artificial intelligence, predictive analytics, or mobile decision support tools, data must be harnessed to solve priority health challenges, especially in resource-constrained settings.

3.2.2.3 Systemic Impact

Promoting the value of health data ensures that Kenya's investments in digital systems yield real dividends such as better care, more timely decisions, and greater health system efficiency. It also helps build a culture where data is seen not as a reporting burden, but as a strategic asset to be protected and productively used.

By embedding these principles, Kenya strengthens its capacity to deliver people-centred, data-driven, and innovation-ready health services.

3.2.3 Governance Objective 3: Prioritising Equity (Kutanguliza Usawa)

Ensure Fairness, Representation, and Shared Benefits from Health Data

3.2.3.1 Objective Overview

At the heart of Kenya's digital health transformation lies a moral imperative: that no one be left behind. The third objective—Kutanguliza Usawa—prioritises fairness and equity in the way health data is governed. It recognises that while data can deepen inclusion, it can also entrench inequality if governance systems ignore structural disparities.

Health data must not only serve the needs of the well-resourced or digitally connected. It must uplift the marginalised, represent the underserved, and empower communities with historically limited influence over health systems.

Equity in data governance means addressing both access and benefit, ensuring that communities contribute to, shape, and fairly receive value from the data their lives generate.

3.2.3.2 Clustered Principles Under this Objective

The principles aligned with this objectivepromote inclusive participation, legal empowerment, and justice in benefit distribution. They include:

Principle 1: Establish Data Rights and Ownership (Kuanza haki za data na umiliki)

Everyone has the right to know, determine, and control how their health data is used. This principle calls for codifying ownership, ensuring informed consent, and recognising community data custodianship through tools such as health data trusts and cooperatives.

Principle 3: Promote Equitable Benefit from Health Data (Kukuza kufaidika kwa usawa na data za afya)

Governance should ensure that the benefits of digital health such asbetter services, smarter planning, and innovations are not concentrated among a few or used to foster discrimination. Equity means sharing data-led improvements with the very communities that generate and contribute data.

3.2.3.3 Systemic Impact

Prioritising equity ensures that digital health tools do not deepen Kenya's urban-rural divide, widen gender gaps, or exclude indigenous, nomadic, or low-literacy populations. It encourages meaningful representation in data design, collection, and use.

It also affirms that governance must go beyond technical rules. It must be responsive to social realities, ensuring that health data strengthens trust, enhances justice, and delivers meaningful impact to all Kenyans.

3.3 Implementing the Principles – Cross-Cutting Considerations

Translating principles into practice is the defining test of a meaningful governance framework. While the three objectives—**Protecting People (Kulinda Watu), Promoting the Value of Health Data (Kukuza Thamani ya Takwimu za Afya),** and **Prioritising Equity (Kutanguliza Usawa)**—provide direction, their effective implementation hinges on how well the health system addresses foundational, cross-cutting factors.

These factors determine whether the principles remain aspirational or become embedded in the everyday behaviours, decisions, and systems of health data governance in Kenya.

3.3.1 Institutional Coordination

Health data governance involves diverse actors across ministries, counties, sectors, and systems. Clear roles, consistent mandates, and harmonised procedures are essential. Implementing the principles requires:

- Strengthening collaboration between the Ministry of Health and the Office of the Data Protection Commissioner (ODPC).
- Establishing structured platforms for coordination across counties, implementing partners, and the Digital Health Agency.
- Clarifying decision rights at each stage of the data lifecycle—from collection to deletion.

3.3.2 Capacity Development

Good governance requires more than good intentions, it demands people with the skills and tools to act. Capacity development is essential across:

- **Technical competencies:** Data stewardship, cybersecurity, analytics, and privacy engineering.
- **Policy literacy:** Understanding of the legal framework among health workers, ICT teams, and data managers.
- **Leadership capabilities:** To champion equity and ethics in digital health decision-making.

3.3.3 Community Engagement and Consent Models

Respect for people begins with transparency and participation. Communities must not be passive data sources but active stakeholders. This entails:

- Designing **consent models** that are culturally appropriate, multilingual, and responsive to varying literacy levels.
- Establishing **community feedback loops** where people can understand how their data is used and voice concerns or preferences.
- Empowering community health units to act as intermediaries between systems and citizens.

3.3.4 Regulatory Harmonisation and Interpretation

As digital health ecosystems evolve, laws and guidelines must stay interoperable and up to date. Implementing the principles will require:

- Guidance notes to harmonise how counties, partners, and facilities interpret and apply national data laws.
- Alignment between the Data Protection Act (2019), Digital Health Act (2023), and cross-border data sharing frameworks.
- Routine legal audits to identify grey zones and adapt quickly to emerging technologies.

3.3.5 Monitoring and Accountability

Principles must be traceable. Without metrics, dashboards, and enforcement mechanisms, ethical commitments may fade into abstraction. Key requirements include:

- Defining measurable indicators for principle-based compliance at national, county, and facility levels.
- Integrating data governance audits into routine health information system (HIS) performance reviews.
- Establishing complaint and redress mechanisms that are accessible to the public and responsive to violations.

In summary, implementing the principles is a dynamic, evolving effort that must be institutionalised across policies, workflows, technologies, and relationships. These cross-cutting enablers are what translate Kenya's values into lasting digital trust.

3.4 Contextualising the Principles for Kenya's Health System

Kenya's health data governance is built on three core principles—**Protecting People (Kulinda Watu), Promoting the Value of Health Data (Kukuza Thamani ya Takwimu za Afya), and Prioritizing Equity (Kutanguliza Usawa)**. These principles were carefully co-developed to reflect the country's unique legal frameworks, digital maturity, and institutional structure, ensuring practical implementation. The following areas were considered for contextualisation:

- **Decentralized health governance:** Counties operate at different levels of digital readiness, requiring adaptable strategies and flexible frameworks for data protection.
- **Cultural & linguistic inclusivity:** Using both English and Kiswahili ensures accessibility, cultural legitimacy, and shared accountability in health data practices.
- **Alignment with digital health priorities:** The framework supports national health strategies like the Digital Health Act (2023), Kenya Health Enterprise Architecture (KHEA), and Universal Health Coverage (UHC), while also addressing regional health needs.
- **Grounded in lived experience:** Developed through consultations with health workers, records officers, communities, researchers and implementors, ensuring relevance in real-world applications.

Why contextualisation matters:

Principles are only effective when they resonate with real people, in real roles, within real systems. Kenya's approach ensures that its health data governance framework is rooted in lived experience, making it practical and accessible for all. By balancing local realities with global best practices, the principles remain adaptable while addressing Kenya's unique landscape.

3.5 Summary

Chapter 3 delves into the Global Health Data Governance Principles and their contextualisation for Kenya. These principles, drawn from international frameworks and best practices, provide the ethical foundation for managing health data in a way that prioritises individual rights, equity, and transparency. The chapter outlines three core principles: Protecting People, Promoting the Value of Health Data, and Prioritising Equity, and explains how these principles guide the governance of health data across Kenya's health ecosystem. Each principle is linked to Kenya's legal and policy frameworks, ensuring they are actionable, lawful, and aligned with national priorities, including those articulated in the Constitution of Kenya (2010), the Data Protection Act (2019), and the Digital Health Act (2023).

The chapter also reflects the importance of localisation in applying global principles, ensuring that Kenya's health data governance is both internationally compliant and tailored to the unique socio-cultural and legal context of the country. The adoption and operationalisation of these principles are framed within the broader goal of creating a secure, ethical, and transparent data governance system that supports innovation while safeguarding individuals' privacy and rights.

As we transition to **Chapter 4,** the focus will shift to the **Leadership, Governance, and Operations** of health data in Kenya. This chapter will outline the institutional structures, roles, and responsibilities that will oversee the implementation of the Health Data Governance Framework (HDGF). It will define the key actors, such as the **Ministry of Health** and **the Digital Health Agency** and describe how they will coordinate the governance of health data across the country, ensuring that the principles outlined in Chapter 3 are effectively operationalised.

4 Health Data Leadership, Governance, and Operations

This chapter outlines:

1. The institutional structures and designated roles responsible for health data governance in Kenya.
2. The specific responsibilities of health data custodians, controllers, processors, and data protection officers.
3. The foundation for governing health data across the lifecycle—ensuring trust, privacy, security, and accountability.

4.1 Introduction

Effective health data governance requires more than just principles—it demands leadership, institutional coordination, and clear roles for implementation. The purpose of this chapter is to define how Kenya's health data governance system will be led, structured, and operationalised in line with national laws and global best practice.

The leadership and governance mechanisms described in this chapter aim to ensure that data is protected, responsibly shared, and ethically used across the health ecosystem. This includes within and across public and private institutions, across counties, and in collaboration with non-state actors.

Kenya's approach is anchored in the Constitution of Kenya (2010) and further operationalised through the Health Act (2017), the Data Protection Act (2019), the Digital Health Act (2023), and other relevant health sector frameworks, policies, and standards. It also aligns with regional and international benchmarks from the World Health Organization (WHO), the African Union (AU), and Regional Economic Communities such as the East African Community (EAC) and Intergovernmental Authority on Development (IGAD).

To accommodate the varying levels of digital maturity across the country, the Framework recognises three main modes of health data system implementation:

Implementation Mode	Definition
 Paper-based systems:	These rely solely on paper as the only tool for managing data.
 Hybrid systems:	These utilize both paper and electronic data systems. The electronic aspects of a hybrid system as typically used in a retrospective data capture manner.
 Fully digital systems:	These rely entirely on digitized systems for data management.

Table 1: Data Systems in Kenya

This chapter outlines the institutional leadership structures, coordination mechanisms, and the specific roles and responsibilities of key actors who will bring the Health Data Governance Framework (HDGF) to life.

4.2 Leadership and Governance

Effective health data governance in Kenya is grounded in the constitutional mandate of the Ministry of Health (MoH) to provide national policy direction, steward the health sector, and ensure coordinated oversight of health service delivery across the Republic. Under the Fourth Schedule of the Constitution, the national government is responsible for health policy, national referral services, and capacity building for counties, while county governments are responsible for health service delivery. This dual structure of authority makes clarity of leadership, governance, and oversight essential for a secure and trusted health data ecosystem.

The Ministry of Health, as the national steward of health policy, is the primary governance authority for health data in Kenya. Its mandate is reinforced through key legislation:

- The **Health Act (2017)** assigns MoH responsibility for establishing norms and standards for health information, protecting personal health data, and guiding the development of an integrated health information system.
- The **Data Protection Act (2019)** requires compliance by all health sector actors and designates MoH among the public bodies responsible for sectorspecific enforcement of privacy safeguards.
- The **Digital Health Act (2023)** provides the overarching legal architecture for digital health governance and establishes the Digital Health Agency (DHA) as the national Health Data Custodian, operating under the policy direction and oversight of MoH.

Within this legal and constitutional framework, health data governance is led by the Ministry of Health, which provides:

a. National Policy Leadership

MoH formulates and issues national policies, regulations, and technical standards for health data governance. It ensures that all actors—public, private, and nonstate—adhere to uniform requirements for data quality, confidentiality, security, interoperability, and ethical use. This includes the development and approval of standards for data collection, reporting, access, retention, and sharing across the health sector.

b. Governance Oversight

MoH oversees the implementation of national health data governance policies by supervising the DHA, guiding county governments, certifying adherence to standards, and ensuring alignment with the Constitution and the national legal framework. This oversight role extends to monitoring compliance, conducting audits, and ensuring accountability across the health sector.

c. Intergovernmental Coordination

Given the devolved nature of health service delivery, MoH provides strategic leadership to ensure coherence between national and countylevel health data systems. County Governments, through County Executive Committee Members (CECMs) for Health, serve as data controllers for countyowned health facilities and are responsible for establishing and maintaining County Health Data Banks, appointing Data Protection Officers, and enforcing adherence to national standards within their jurisdictions.

MoH works with counties through constitutionally established intergovernmental mechanisms to ensure that health data governance is harmonised nationwide and supports continuity of care, surveillance, planning, and service quality.

d. Coordination with Partners through Existing Partnership Mechanisms

While Kenya's health sector benefits from robust collaboration with development partners, civil society, and private actors, partnership structures are not governance organs. Instead, they serve as coordination mechanisms that support alignment, resource mobilisation, and technical collaboration.

MoH provides oversight of health sector partner engagement using the existing Health Sector Partnership Frameworks. These mechanisms facilitate sectorwide dialogue, technical collaboration, and joint planning but do not replace MoH's statutory governance authority over health data.

e. DHA as an Implementing Agency Under MoH Supervision

The Digital Health Agency, established by

the Digital Health Act (2023), functions as the technical implementing institution for digital health systems and the custodian of national health data. DHA is responsible for developing, operating, and maintaining the Comprehensive Integrated Health Information System (CIHIS), certifying digital health solutions, and enforcing national interoperability and data governance standards under the policy direction and regulatory oversight of MoH.

f. CountyLevel Leadership

Counties, as custodians of service delivery data, implement national policies within local health systems. Their responsibilities include:

- enforcing national data governance standards at facility level
- ensuring secure management of county health data
- operationalising County Health Data Banks
- appointing Data Protection Officers
- supporting compliance with reporting, access, and data sharing requirements

Their leadership ensures that health data governance is fully embedded in realworld service delivery across all public and private facilities operating within county boundaries.

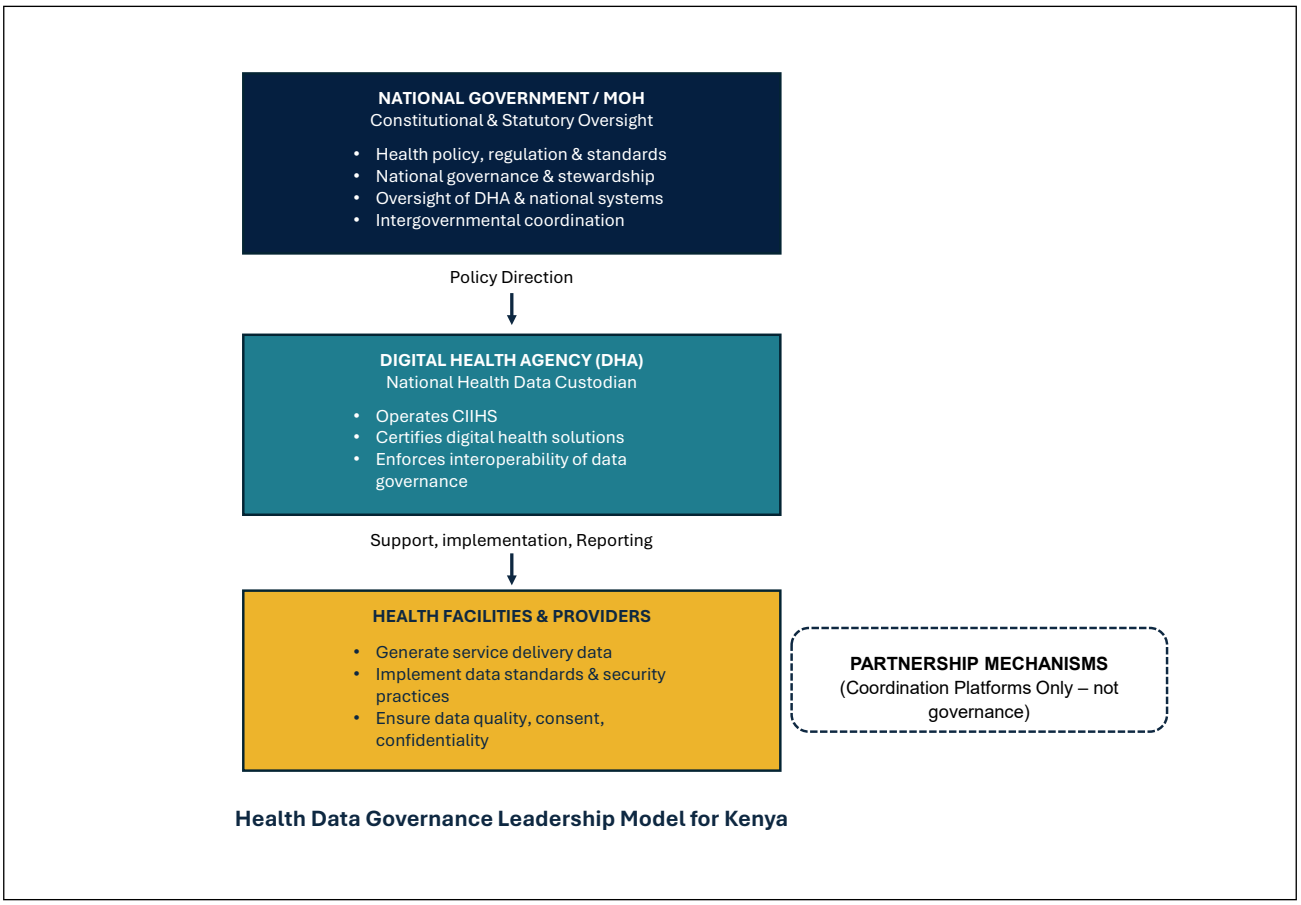


Figure 6: Health Data Governance Leadership Model for Kenya

4.3 The Digital Health Agency

The Digital Health Agency was established under the Digital Health Act, 2023 to serve as the institutional anchor for Kenya's digital health infrastructure. It plays a central role in implementing and sustaining the Health Data Governance Framework (HDGF) and is the designated custodian of all health data in the country.

The Agency is mandated to:

- Develop, operationalise, and maintain the Comprehensive Integrated Health Information System (CIHIS)
- Coordinate the management of core digital systems and infrastructure required for seamless health data exchange
- Support national priorities on health data use, protection, and innovation

These responsibilities are carried out in consultation with other statutory authorities and relevant government agencies to establish a single source of truth on key national health registries—including clients, facilities, providers, products, and technologies.

4.3.1 Functions of the Digital Health Agency

As outlined in the **Digital Health Act, 2023**, the Agency performs the following key functions to support effective governance of health data:

a. Promote the adoption of digital health best practices and standards that enable secure data exchange
b. Establish systems for shareable and portable personal health records and ensure health data portability
c. Facilitate the collection and analysis of data to inform health policy, strategy, and research
d. Promote the development and certification of enterprise-class digital health solutions
e. Strengthen existing health information systems to align with prescribed standards and ensure integration into the national CIHIS
f. Develop and implement the infrastructure for secure health information exchange
g. Support the design and enforcement of interoperability standards across systems and platforms
h. Collaborate with counties and statutory agencies to maintain the technological backbone for digital health services
i. Mobilise financial and technical resources to advance digital health investment and scale-up
j. Advise the Cabinet Secretary on matters related to digital health

Summary: As custodian of Kenya's national health data, the Digital Health Agency is the principal implementer of digital health governance. It bridges health sector policy, digital infrastructure, and data rights, enabling an ecosystem where information flows securely and equitably to drive improved health outcomes.

4.4 Roles and Responsibilities

To effectively implement the Health Data Governance Framework (HDGF), specific roles and responsibilities have been defined for key actors across the health sector. These roles reflect statutory mandates, promote coordinated governance, and ensure accountability at all levels of the health data ecosystem.

4.4.1 Health Data Custodian

The Digital Health Agency is designated by the Digital Health Act, 2023 as the official custodian of all health data in Kenya.

As the Health Data Custodian, the Agency is responsible for:

a. Maintaining a register of all health data controllers and processor
b. Keeping an inventory of health data assets held by these actors
c. Ensuring health data controllers submit data in the approved formats
d. Maintaining the National Health Data Bank and fulfilling duties under the Digital Health Act
e. Providing authorised access to health data in accordance with applicable laws
f. Retaining health data for a minimum of 20 years, or as specified in this Framework
g. Applying security safeguards—firewalls, encryption, and access controls—to prevent unauthorised access or misuse
h. Maintaining a public portal for health data controllers and processors to access SOPs and templates
i. Making selected aggregate data publicly accessible in standardised formats
j. Ensuring compliance with this Framework by all data controllers and processors

4.4.2 Health Data Controller

A **health data controller** refers to any individual, institution, agency, or legal entity that determines the purpose and means of processing health data.

Responsibilities include:

a. Registering as a data controller with the Office of the Data Protection Commissioner (ODPC) if handling sensitive personal data
b. Notifying the Digital Health Agency of the type of health data held
c. Ensuring health data processors under their jurisdiction are registered with the ODPC
d. Appointing a Data Protection Officer (DPO) to oversee data protection compliance
e. Complying with the principles of this Framework throughout the data lifecycle
f. Using certified digital health solutions for data management
g. Applying the highest standards of data security, confidentiality, and integrity
h. Conducting regular data quality assessments using tools approved by the Digital Health Agency
i. Ensuring all processors under their jurisdiction meet reporting obligations to MoH
j. Complying with this Framework and relevant legislation
k. Providing and sharing health data in accordance with this Framework and relevant laws

4.4.3 County Executive Committee Members for Health (CECMs)

As health data controllers for county owned health facilities, and implementers of health at the county level, CECMs are responsible for:

a. Fulfilling all duties of health data controllers in their jurisdiction
b. Establishing and administering County Health Data Banks
c. Performing all responsibilities outlined under Sections 26–28 of the Digital Health Act, 2023
d. Ensuring data in County Health Data Banks is managed in line with this Framework

4.4.4 Health Data Processor

A health data processor is any individual or organisation authorised to process health data on behalf of a health data controller.

Responsibilities include:

a. Registering with the ODPC if processing sensitive personal data
b. Notifying the Digital Health Agency of the category of data held
c. Complying with this Framework throughout the data management lifecycle
d. Using only certified digital health solutions
e. Applying stringent data security and privacy safeguards
f. Conducting regular data quality assessments using standards set by the Agency
g. Fulfilling all reporting obligations using approved MoH platforms

4.4.5 Data Protection Officers (DPOs)

A Data Protection Officer (DPO) is a designated individual with relevant qualifications and experience in data protection and health data management. Each data controller or processor handling sensitive health data must appoint a DPO, whose responsibilities include:

a. Developing and implementing internal data protection policies and procedures
b. Conducting impact assessments and audits
c. Responding to data subject queries
d. Training staff on privacy and data protection
e. Liaising with the ODPC and Digital Health Agency
f. Reporting data breaches and associated mitigation actions
g. Leading internal awareness and compliance efforts

At the county level, a member of the County Health Management Team (CHMT) shall be designated to fulfil the DPO role.

4.4.6 Health Data Subjects

A health data subject is the individual to whom the health data relates. Under the Data Protection Act, 2019, the health data subject is the legal owner of their personal health data.

Rights of the data subject include:

1. The right to be informed of how their data is used
2. The right to control access to their data
3. The right to object to the processing of their data
4. The right to correct inaccurate or misleading data
5. The right to delete false or misleading data
6. The right to be forgotten, subject to applicable laws and policies

These rights reflect the core principle of protecting people (Kulinda Watu) and ensure that individuals remain central to Kenya's health data governance system.

These clearly defined roles ensure a coordinated, legally compliant, and people-centred approach to health data governance—where institutions are accountable, and individuals' rights are upheld throughout the data lifecycle.

4.5 Summary

Chapter 4 outlines the **Leadership, Governance,** and **Operations** structures essential for the successful implementation of the Health Data Governance Framework (HDGF) in Kenya. It defines the institutional roles and responsibilities necessary to ensure effective data governance across the health sector. The chapter introduces key actors such as the Ministry of Health, the Digital Health Agency, and various data controllers and processors, explaining their mandates and how they will collaborate to govern health data at national, county, and facility levels.

The chapter emphasizes the importance of coordination and accountability, highlighting how the governance structures will be integrated into Kenya's health data ecosystem. It further explores the role of the Digital Health Agency as the custodian of health data and its responsibility in overseeing data management practices, from data collection to processing and sharing. The governance framework is anchored in Kenya's legal commitments, ensuring that all actions align with national laws and international standards.

With the leadership and operational structures in place, the next logical step is to focus on data management. **Chapter 5** will delve into the **health data management** lifecycle, outlining the stages of data collection, processing, retention, and disposal. It will highlight the criteria and best practices for managing health data while ensuring security, privacy, and compliance with relevant laws, providing a comprehensive view of how data will be handled responsibly throughout its lifecycle.

5 Health Data Management

This chapter outlines:

1. How health data is collected, processed, accessed, retained, and disposed across its lifecycle.
2. The governance, legal, and ethical safeguards that apply to each stage of the data management process.
3. Standards that ensure health data remains secure, private, confidential, and of high quality.

Introduction

Health data management plays a pivotal role in ensuring that health data is used effectively and responsibly throughout its lifecycle. This chapter outlines the comprehensive approach to managing health data in Kenya, from its collection and processing to retention and destruction, underpinned by strong governance, legal, and ethical safeguards. The goal is to ensure that health data remains secure, private, confidential, and of the highest quality while adhering to national and international standards.

The management of health data is not only about maintaining accuracy and completeness, but also about protecting the rights of individuals and fostering trust within the health system. The framework presented here outlines how data is collected, processed, validated, and shared, ensuring that all activities comply with Health sector regulations, the DPA, 2019 as well as the broader Health Data Governance Framework (HDGF) as shown in Figure 7 below.

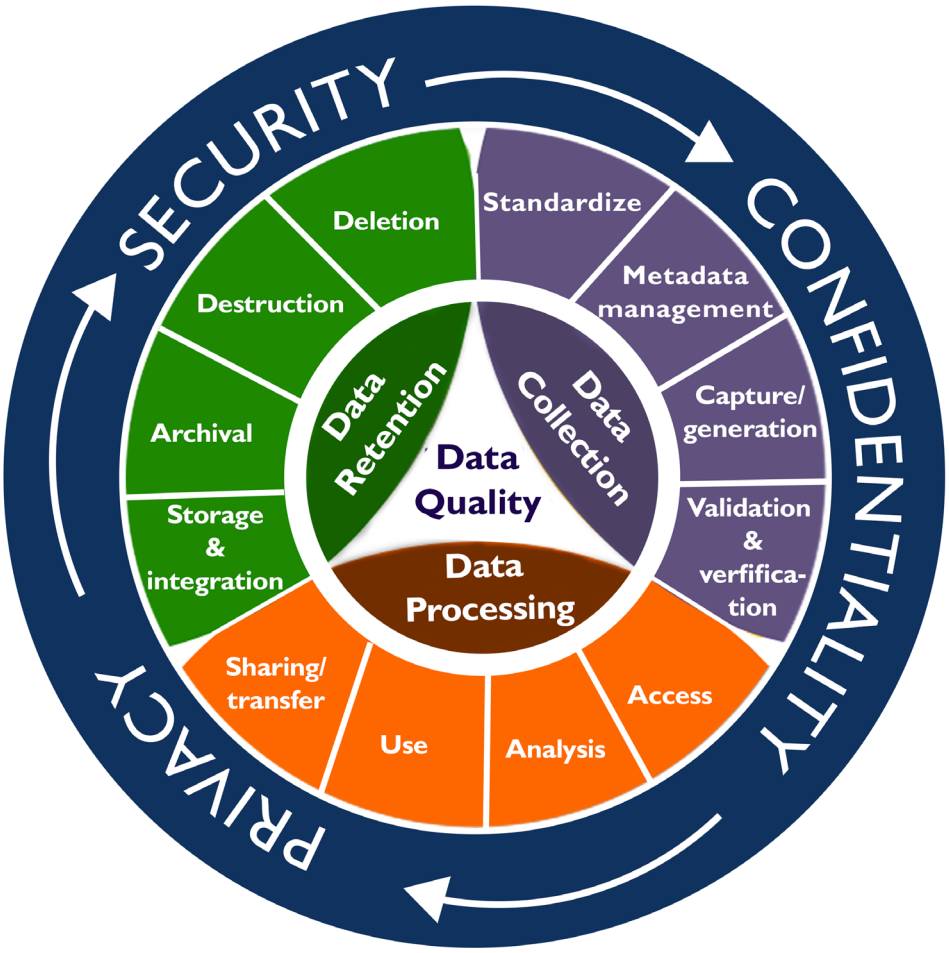


Figure 7: Data Management Approach.

Key Principle:

Only collect what is necessary; minimising risk and upholding the rights of the data subject.

5.1 Data Collection

Health data collection is the entry point of the data lifecycle. It involves systematically identifying, defining, and gathering data from individuals, institutions, and systems. The collection process must be transparent, consented where required, and purpose driven. It includes key activities such as:

- Standardisation of data elements and indicators,
- Metadata management via the National Health Data Dictionary (NHDD),
- Capture and generation from sources such as EMRs, medical devices, public health surveillance, and research,
- Validation and verification to ensure data quality dimensions such as accuracy, completeness, and reliability are met.

As illustrated in Figure 5, data collection sits within a broader cycle of data management—reinforced by principles of security, confidentiality, privacy, and a core commitment to data quality.

5.1.1 Metadata Management

Metadata—data about data—is foundational to effective health information management. In Kenya, metadata management is operationalised through the National Health Data Dictionary (NHDD), also referred to as the National Health Terminology Service.

The NHDD is developed, maintained, and governed by the Digital Health Agency, and serves as a shared national resource that ensures semantic consistency across all health data systems. It defines standardised data elements, terminologies, classifications, code systems, and value sets for use in both public and private health sector operations.

All clinical and public health data collected through Point-of-Care Systems (POCs) must be mapped to the NHDD, ensuring that:

- Variables are unambiguous and consistently interpreted
- Minimum datasets are defined in consultation with MoH departments
- Metadata remains interoperable across systems and borders

The Health Act, 2017, requires these minimum datasets to be reviewed every three years, ensuring their continued relevance and alignment with sector needs.

Key Safeguard: While metadata does not contain sensitive personal information, it is considered a critical national asset and is therefore subject to governance provisions outlined in the HDGF.

5.1.2 Data Standardisation

Data standardisation ensures that the information collected across diverse systems is consistent, comparable, and interoperable. It is the foundation for accurate aggregation, reporting, and decision-making across Kenya's health system.

Standardisation in the Kenyan context involves:

- Adapting and localising international standards, particularly those issued by the World Health Organization (WHO) and other global partners.
- Promoting the adoption of the WHO SMART Guidelines, which provide structured, evidence-based standards for digital health.
- Ensuring uniform processes, indicators, and data elements across programs and platforms.
- The Digital Health Agency is mandated to:
- Facilitate the adoption and enforcement of approved data standards
- Promote and maintain the National Health Data Dictionary (NHDD) as the central reference point for all terminologies and value sets
- Link the NHDD with international terminology services, enabling cross-border semantic interoperability

All health sector actors—public and private—are required to normalise their data to the

NHDD, ensuring compatibility and reducing fragmentation across platforms.

National Shared Service:

The NHDD is designated as an essential digital infrastructure for Kenya's health sector—critical for real-time analytics, program monitoring, and innovation.

5.1.3 Data Capture and Generation

Health data can enter the system through two primary pathways: data capture and data generation.

5.1.3.1 Data Capture

This refers to the recording of information from existing sources, including:

- Paper-based tools and registers
- Electronic Health Records (EHRs) and Electronic Medical Records (EMRs)
- Medical devices and diagnostics equipment
- Health surveys and censuses
- Public health surveillance systems
- Administrative and logistics information systems

Data capture ensures that routine health service interactions and operations are recorded accurately and systematically, forming the basis of patient care and service delivery monitoring.

5.1.3.2 Data Generation

Data generation refers to the creation of entirely new datasets through:

- Clinical trials and experimental research
- Genomic sequencing or molecular profiling
- Advanced analytics involving the Internet of Things (IoT), Artificial Intelligence (AI), and Machine Learning (ML)
- Wearables, sensors, and other emerging technologies

Both processes—capture and generation—must uphold the core tenets of health data governance: accuracy, reliability, security, compliance, and traceability.

Governance Mandate:

All entities collecting or generating data are considered either health data controllers or processors and must comply with the provisions of the Data Protection Act (2019), Digital Health Act (2023), and this Framework.

5.1.4 Data Inventory & Accessibility

A well-organized **data inventory** ensures health data is identified, classified, and tracked for secure and efficient use. By documenting data sources—including databases and cloud storage—organizations improve accountability and regulatory compliance while supporting seamless data management across digital, hybrid, and manual systems.

Data accessibility ensures collected and stored health data is usable, available, and secure. It balances availability for authorized users, usability for structured interpretation, and security to protect confidentiality while enabling interoperability. Optimizing inventory and accessibility supports informed decision-making, seamless data sharing, and actionable insights, strengthening Kenya's health data governance.

To support data inventory and accessibility, Health Data Controllers and Processors are required to:

- Maintain a comprehensive dataset inventory with up-to-date data dictionaries
- Describe data coverage, programmatic relevance, and availability for internal and external use
- Ensure the inventory is accessible to county departments of health, relevant stakeholders, and the MoH

5.1.5 Validation and Verification

Validation and verification are essential quality assurance steps in the health data lifecycle. They ensure that data collected across Kenya's health system is accurate, consistent, and fit for use at all levels—from community health units to national programs.

Definitions:

- **Validation** confirms that data values are within expected ranges, formats, and structures.
- **Verification** checks whether the data reported accurately reflects the reality on the ground (e.g., comparing register entries with system reports).

These activities should be systematic, standardised, and documented, with a focus on strengthening data trustworthiness for both operational and strategic use.

Responsibilities:

- The Ministry of Health will develop and periodically update national Data Quality Assurance (DQA) Guidelines to support uniform application across programs and counties.
- National and county governments are mandated to:
  - Organise regular data quality assessments (DQAs)
  - Facilitate periodic data validation and verification audits
  - Ensure findings from these activities inform corrective action plans

Wherever possible, automated DQA tools and processes should be used to enhance efficiency and reduce human error. All verification and validation exercises must adhere to the definitions and responsibilities assigned to health data processors in this Framework.

DQA Output:

Each assessment must result in a report detailing findings, recommended corrective actions, and, where applicable, justifications for any data modifications made.

5.2 Data Processing

Data processing refers to the structured transformation of raw health data into usable information. This process enables decision-makers to draw meaningful insights for patient care, public health surveillance, research, and health system strengthening.

Processing activities include:

- Data cleaning, standardisation, and transformation,
- Integration across systems,
- Aggregation and disaggregation,
- Analysis, visualisation, and reporting.

Processing Mandate:

The **Ministry of Health (MoH)** and the **Digital Health Agency** are jointly responsible for:

- Ensuring health data is processed in a manner that promotes innovation, learning, and system-wide improvement,
- Facilitating access to processed data for valid public health purposes,
- Applying safeguards that protect individuals and communities from harm.

Guiding Principle:

Data processing should always aim to maximise public benefit while minimising risks—particularly when dealing with sensitive personal data.

Additionally, data controllers and processors must apply the Data Protection Impact Assessment

(DPIA) process atleast annualy, as guided by the Office of the Data Protection Commissioner (ODPC), to assess and mitigate processing risks, especially when using new or high-risk technologies..

5.2.1 Planning and Strategic Alignment

Effective health data processing must be guided by clear national goals and aligned with sector-wide strategic priorities. In Kenya, these priorities are defined in the **Kenya Health Sector Strategic Plan (KHSSP) 2024–2028,** the **Kenya Health Policy (2014–2030),** and national disease control strategies.
At a minimum, data processing and use activities must support:

- Tracking progress toward Universal Health Coverage (UHC)
- Monitoring health system performance
- Informing disease surveillance, emergency response, planning, and policy
- Strengthening research and innovation across health programs

Institutional Planning Responsibilities

- The Ministry of Health (MoH), in collaboration with county governments and development partners, will coordinate the annual work planning process for data use activities.
- Every three years, the MoH will define core health indicators and issue standardised indicator reference guides.
- Disease-specific programs and surveillance initiatives will develop data use business cases and analysis plans that reflect health priorities.

Public Health Utility:

A subset of curated datasets should be made available to support shared services, national reporting, research, and policy development—consistent with privacy safeguards.

5.2.2 Data Analysis and Interpretation

Data analysis is a critical function of health data processing. It transforms raw data into actionable insights that support decision-making, inform public health strategies, and improve service delivery.

Analysis should be guided by the principle that data, first and foremost, reflects records of care, and should be used to improve outcomes for individuals and populations.

Responsible Actors:

Data analysis is a shared responsibility between:

- The Ministry of Health and its technical programs
- County departments of health
- Health facilities and data controllers
- Academic and research institutions
- The Digital Health Agency, which supports national analytic capabilities and tool development

These stakeholders are encouraged to:

- Develop regular data analysis plans and use cases
- Identify key reporting needs
- Promote evidence-informed program improvements
- Define research priorities in collaboration with data producers and custodians

Enabling Innovation:

Ethical and equitable application of Artificial Intelligence (AI) and Machine Learning (ML) should be encouraged—particularly for forecasting, risk prediction, and health system optimisation.

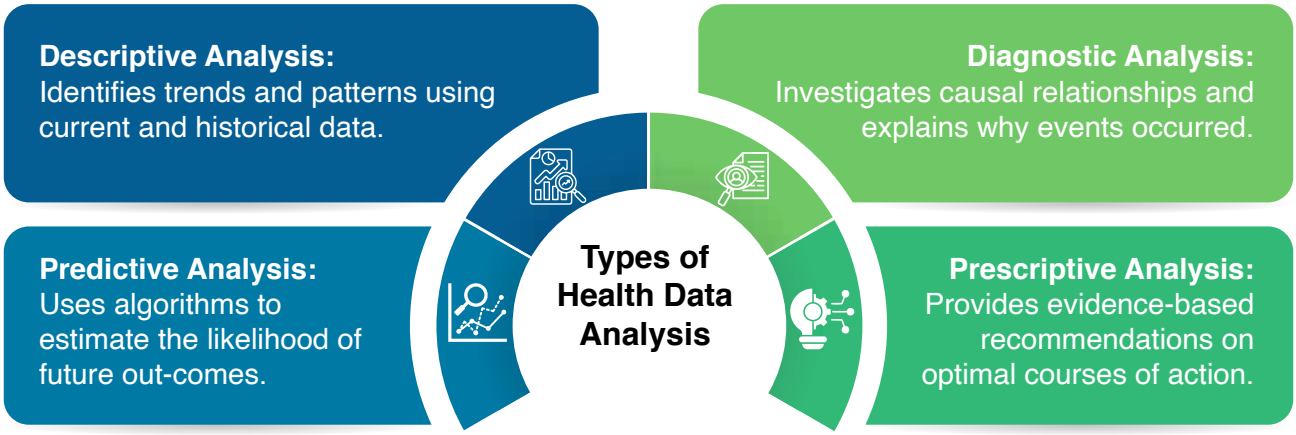


Figure 8: Types of Health Data Analysis

Best Practice:

All analyses should be reproducible, documented, and securely stored. When possible, open-source tools and dashboards should be used to promote transparency and access.

5.2.3 Use of Emerging Technologies for Data Processing

The rapid evolution of digital tools is reshaping how health data is processed, interpreted, and used in Kenya. Technologies such as Artificial Intelligence (AI), Machine Learning (ML), and the Internet of Things (IoT) present significant opportunities to strengthen clinical decision-making, enhance public health surveillance, and unlock predictive and personalised care. However, these innovations must be applied in ways that are responsible, ethical, and rights-based, in line with the Digital Health Act (2023) and the Data Protection Act (2019).

Guiding Principles for Responsible Use of AI/ML in Health Data

All actors deploying emerging technologies for health data processing must adhere to the following principles:

1. **Protect Human Autonomy**
   Ensure that technology supports—not replaces—human decision-making. Clinical oversight, transparency, and informed consent must remain central.

2. **Promote Human Well-being and Public Interest**
   Technologies must meet regulatory standards for safety, accuracy, and effectiveness. Continuous monitoring is required to ensure that tools remain beneficial over time.

3. **Ensure Transparency and Explainability**
   Systems must be intelligible to developers, regulators, and end-users. Clear documentation should describe how algorithms function and reach decisions.

4. **Foster Responsibility and Accountability**
   Developers and implementers must ensure clear lines of accountability. There should be provisions for oversight, performance monitoring, and redress where harm occurs.

5. **Ensure Inclusiveness and Equity**
   Technologies must be inclusive in design and deployment. Stakeholders from diverse backgrounds—including marginalised populations—should be consulted.

6. **Promote Responsiveness and Sustainability**
   Digital solutions must be adaptable to changing health system needs and sustainable over time. This includes interoperability, maintainability, and resource availability.

Ethical Safeguard: Any use of AI/ML in health must be preceded by a Data Protection Impact Assessment (DPIA), aligned with ODPC guidelines.

5.2.4 Data Access and Sharing

Accessing and sharing health data is essential for individual care, health system performance, research, and public health protection. However, these activities must be governed by strong ethical, legal, and procedural safeguards to uphold privacy, security, and trust.

This Framework recognises four primary purposes for which health data may be accessed or shared:

- Individual benefit and care coordination
- Program improvement and service delivery
- Research and innovation
- Public health policy and planning

Access and sharing must comply with the **Access to information Act (2016), Data Protection Act (2019), Digital Health Act (2023),** and relevant ethical review and data governance mechanisms.

Access and sharing are not unrestricted rights—they are regulated privileges that must serve public interest and protect personal rights.

Principles of Health Data Access

As illustrated in Figure 9, all data access and sharing must be guided by the following five principles:

1. **Transparency** – Who is accessing the data, how, and for what purpose must be clearly documented.
2. **Consent** – Data subjects must be informed and, where applicable, provide explicit consent for data access.
3. **Security** – Data must be protected from unauthorised access through strong technical and organisational controls.
4. **Purpose Limitation** – Data should only be accessed for specific, legitimate purposes.
5. **Accountability** – Access logs, audit trails, and oversight mechanisms must be maintained.

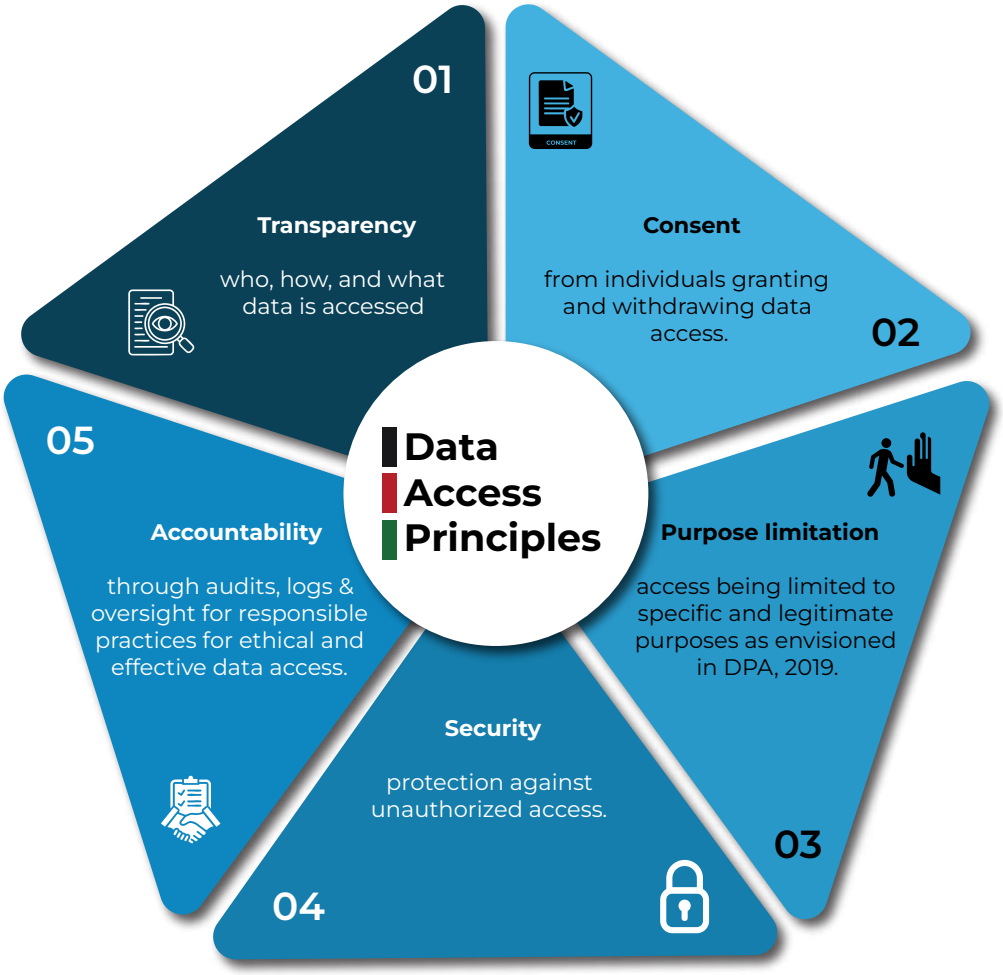


Figure 9: Principles of Data Access

Access Levels and Authorised Users

Access to health data is defined by user type, data sensitivity, and intended use:

User Type	Examples	Access Requirements
Internal Authorised Users	MoH and county health teams, facility owners	Role-based access for service delivery, planning, and policy
Registered & Authenticated Users	Healthcare providers, patients, health information officers	Requires consent (if accessing sensitive data); access is logged
Limited Access Users	NGOs, researchers, development partners	Requires data request, approvals, and data-sharing agreements
Public Users	General public	Access to aggregated, anonymised open data (e.g., dashboards, reports)

Table 2: Access Levels and Authorised Users

Sensitivity-Based Access Control

Sensitivity Level	Description	Access Control
High	Contains Personally Identifiable Information (PII)	Strict controls, role-based access, encryption
Medium	De-identified or pseudonymised data	Conditional access via data-sharing agreements
Low	Aggregated or publicly available data	Freely accessible, no individual identifiers

Table 3: Sensitivity-Based Access Control

Consent Requirements:

Consent must be obtained when accessing identifiable data for secondary use (e.g., research). For primary service delivery and public health, notification to the health client stating the location and purpose suffices under the DHA, 2023.

5.2.4.1 Governance of Data Access

The governance of data access ensures that only authorised individuals and entities are permitted to interact with health data—and only for purposes aligned with Kenya's laws, policies, and this Framework. Access must be granted on a need-to-know basis, proportionate to the user's role and the sensitivity of the data requested.

Access Categories and Governance Requirements

a. Internal Authorised Users
Includes national and county health officials, facility managers, and program coordinators.

- Access is granted for policymaking, planning, monitoring, and service delivery.
- Access should follow standard operating procedures (SOPs), and logs must be maintained.

b. Registered and Authenticated Users Includes:

- **Healthcare providers** accessing Shared Health Records (SHR) for patient care (with automated and logged notification to data subject as required under the DHA, 2023) ,
- **Patients and data subjects** accessing their personal data through patient portals. If the required data is not available in the patient portal, health data subjects may submit additional data access requests directly to the health facility. Should the health facility be unable to provide the requested data, the data subject may escalate the request to the county health data controller, and subsequently to the health data custodian if necessary.
- **Other data handlers** such as accredited health information officers and ICT personnel. The access of data for these handlers should be in line with regulatory requirements and Principle of data minimisation should be employed.

Note: Consent is required when accessing sensitive personal data for purposes beyond service delivery

If access is denied at a facility level, the request may be escalated to the County Health Data Controller, and subsequently to the Digital Health Agency.

c. Limited Access Users
Includes NGOs, development partners, advocacy groups, and researchers.

- Formal data requests must be submitted using standardized templates.
- Ethical review may be required by an Institutional Review Board and regulatory bodies such as the National Commission for Science, Technology, and Innovation (NACOSTI).
- Data-sharing agreements must be signed, with a clear justification for intended use.
- Approval is granted by health data controllers or the Digital Health Agency, ensuring compliance with governance policies.

d. Publicly Available Data Users
Includes journalists, students, and members of the general public.

- Access is restricted to aggregated, de-identified datasets (e.g., dashboards, reports).
- No access is granted to data containing PII.

Data Access Conditions

All access requests must meet one or more of the following conditions:

1. Clearly defined purpose (aligned with public health or service delivery).
2. Minimum necessary data requested to fulfil the stated objective.
3. Compliance with consent and notification protocols.
4. Documentation and approval of access via SOPs and data-sharing agreements.

Transparency and Traceability:

All access must be logged, traceable, and subject to periodic audit by health data custodians and the ODPC.

5.2.4.2 Governance of Data Sharing

Data sharing refers to the controlled transfer of health data from one entity (or actor) to another for lawful purposes such as service delivery, research, program monitoring, or public health response.

Unlike access—which is typically internal—sharing involves movement of data between systems, actors, or jurisdictions. It must therefore be explicitly governed through agreements, documentation, and adherence to the principles of consent, proportionality, and accountability.

Foundational Requirements

- All data sharing must comply with the Data Protection Act (2019) and the Digital Health Act (2023).
- Any transfer involving Personally Identifiable Information (PII) or sensitive personal health data requires either:
  - Consent from the data subject (unless otherwise provided for in law), or
  - A legal exception defined in legislation (e.g., public health surveillance under the Public Health Act (2012))

Data Sharing Agreements (DSAs)

Any sharing of data outside the originating institution or system requires a **Data Sharing Agreement,** which must include:

- Scope of data to be shared
- Purpose and intended use
- Duration and terms of use
- Confidentiality, security, and ethical provisions
- Data destruction or return clause upon project conclusion
- Provisions for monitoring and enforcement
- Responsibilities of each party

Note: Sharing must remain within the boundaries of the original consent under which the data was collected and terms set in the data sharing agreement. If the intended use changes, new consent or

authorisation is required (new DSA is undertaken reflecting changes).

Data Sharing Conditions

The Framework stipulates that shared data:

- **Must only be used** for the purpose stated in the request or agreement,
- **Cannot be reshared or repurposed** without further authorization through a DSA,
- **Must be anonymised or pseudonymised,** unless explicit consent and lawful justification for identifiable data is obtained,
- **Should be the minimum data necessary** for the intended function.

Security Reminder:

All shared data must be transmitted through secure channels with strong encryption, audit trails, and access logs.

Anonymisation and De-identification Standards

Before sharing, PII must be removed or transformed using:

- Removal of direct identifiers (e.g., name, ID number)
- Generalisation (e.g., age ranges instead of birthdates)
- Aggregation to higher-level units (e.g., county-level data)

In the event of inadvertent identification, the data requester must immediately:

1. Refrain from recording or using the identified data
2. Notify the Digital Health Agency and the ODPC
3. Cooperate fully in mitigation and compliance follow-up

5.2.4.3 Cross-Border Data Access, Sharing, and Use

Kenya's participation in regional and global health initiatives necessitates the secure and lawful sharing of health data across national borders. This may arise in the context of disease surveillance, health research, health tourism, or international cooperation under frameworks such as:

- Africa CDC/AU Health Information Exchange Guidelines
- IGAD Regional Health Data Sharing and Protection Policy
- WHO International Health Regulations (IHR)

Principles for Cross-Border Data Exchange

All cross-border data sharing must adhere to Kenya's domestic legal framework—primarily:

- The Data Protection Act, 2019 (DPA)
- The Digital Health Act, 2023 (DHA)
- Any bilateral or multilateral agreements Kenya is a party to such as International Health Regulations, 2005 and others

Key Principle:

No cross-border data transfer should occur unless the receiving country or institution demonstrates an equivalent or adequate level of data protection.

Governance Requirements

Cross-border data transfers must:

1. Be supported by a formal **Data Sharing Agreement (DSA)** stipulating:
   - The roles, responsibilities, and data protection measures of all parties,
   - Purpose limitation, retention timelines, and conditions for re-use or third-party access,
2. Use **secure, auditable, and encrypted channels** for transmission

3. Adhere to Kenya's legal requirements and clearance mechanisms
   - Transfers of sensitive personal data to foreign jurisdictions must only occur if the recipient country provides an equivalent level of protection, as determined by the ODPC,
4. Be consistent with Kenya's foreign policy, public interest considerations.

Permitted Use Cases

Cross-border sharing is permitted for:

- Public health surveillance and outbreak response
- Health research approved by a recognised Institutional Review Board (IRB) and the National Commission for Science, Technology, and Innovation (NACOSTI)
- Health tourism or patient referral pathways as defined under Section 47 of the Digital Health Act, 2023

Sensitive Data Alert:

If PII is to be included in a cross-border data transfer, explicit consent must be obtained from the data subject—unless exempted by law.

5.2.4.4 Data Portability

Data portability is the right of a data subject to receive their personal health data in a structured, commonly used, and machine-readable format—and to transmit it to another system, service, or provider without hindrance.

This right is enshrined in both the:

- Data Protection Act (2019), and
- Digital Health Act (2023) (Section 31), which mandates patient access to and control over their personal health records.

Purpose and Significance

Data portability:

- Promotes continuity of care when patients move between providers or regions
- Enhances personal autonomy and control over health decisions
- Facilitates innovation and competition by enabling interoperable health services
- Supports regional integration and mobility across public and private health systems

Conditions for Portability

Health data controllers must ensure that:

1. Data is provided in standardised, machine-readable formats (e.g., HL7 FHIR, JSON, XML)
2. Patients are able to access and download their data through secure, user-friendly interfaces (e.g., patient portals)
3. Requests for data portability are responded to within 72 hours, with either the data or a valid explanation for denial
4. Transfers occur over secure, encrypted channels that maintain confidentiality, integrity, and auditability
5. Informed consent is obtained from the data subject before initiating any third-party data transmission

Note: Portability applies to all data that a person has provided or that has been generated about them during service delivery—subject to security and feasibility constraints.

5.3 Data Retention

Data retention refers to the policies, timelines, and technical measures that govern how long health data is stored—and how it is eventually archived or destroyed. In Kenya, all health data—regardless of format—must be retained in accordance with this Framework, the Digital Health Act (2023).

Retention practices must balance:

- Operational need for continuity of care
- Legal obligations under public health, employment, and archival laws
- Data minimisation principles to prevent excessive storage of sensitive data

Key Principle:

Retain what is necessary, secure it while stored, and dispose of it responsibly when no longer required.

5.3.1 Data Storage

Health data storage must ensure long-term accessibility, security, and compliance. It includes local and cloud-based systems.

Storage Requirements:

- At least one serving copy of health data must be physically stored in Kenya (data localisation requirement).
- Storage facilities must maintain perpetual access to data for authorised health providers and institutions.
- If health data—especially PII—is stored outside Kenya, the data controller must:
  - Notify the Office of the Data Protection Commissioner (ODPC)
  - Justify that the receiving country meets Kenya's data protection adequacy standards
  - Ensure patient access rights and local backups remain intact

Security Safeguard:

All health data must be encrypted at rest and in transit using industry-standard protocols.

5.3.1.1 Cloud Computing and Localisation of PII Data

Cloud computing providers handling health data must:

1. Store sensitive personal data in Kenya, or provide a local backup copy if hosted abroad
2. Meet the minimum safeguards set by the ODPC and MoH, including:
   - Strong encryption
   - Role-based access controls
   - Secure disaster recovery and backup protocols
   - Continuous auditing and monitoring
   - Legal clearance for offshore hosting of PII
3. Comply with additional international standards where applicable (e.g., GDPR, HIPAA)

Health Cloud providers must work with the Digital Health Agency to ensure all hosted systems are certified and integrated into national health architecture.

5.3.2 Data Archival

Data archival refers to the secure, long-term preservation of health data that is no longer in active use but must be retained for legal, clinical, administrative, or historical purposes. Archiving enables continuity of care, research, auditing, and accountability—while supporting decongestion of operational systems.

5.3.2.1 Archival Responsibilities

Health data controllers must:

1. Retain minimum essential data in the Shared Health Record (SHR), as defined by the Digital Health Agency
2. Maintain an internal record of the archival process (metadata, formats, timeline)
3. Submit a copy of the archival record to the Digital Health Agency and any other relevant authority
4. Notify data subjects at least seven (7) days before their data is archived

If a controller lacks archival capacity, they must transfer data to the **County Health Data Bank,** managed by the County Executive Committee Member (CECM) for Health.

Security Requirement:

All archival systems must meet national and international data security standards for confidentiality, integrity, and availability.

5.3.2.2 Archival Methods

a. Manual Data Archiving

Manual data archiving refers to the process of storing physical records in a secure and organized manner for future reference. In Kenya, the **Public Archives and Documentation Act (Cap 19)** governs the management and preservation of public records. Within the health sector;

- Paper-based records must be stored for **at least 30 years** from the creation date
- Proper indexing and secure storage are mandatory

b. Digital Data Archiving

Digital data archiving refers to the process of storing electronic records in a secure and organised manner for future reference. In Kenya, the DHA, 2023 governs the management and preservation of digital health data. The Act requires that:

- Personally identifiable information (PII) must be anonymised or pseudonymised before archiving
- Storage must prevent unauthorised access, destruction, or modification
- Archived datasets must remain searchable, traceable, and retrievable for permitted use
- Shall retain the minimum data elements as specified in the Shared Health Record.

Retention Timelines by Data Type

Data Type	Minimum Retention Period
General Health Records	20 years after last interaction or 8 years after death
Maternity Records	25 years after birth of last child
Immunisation Data	Based on anticipated future need; subject to special case review
Research Data	3 years after publication; 15 years for clinical trials; permanent for gene therapy
Occupational Health Records	Duration of employment + 30 years
Litigation-related Rec-ords	Until all investigations and legal matters are resolved and closed

Table 4: Retention Timelines by Data Type

Audit Requirement:

Archived data must be reviewed annually to ensure compliance with retention and security standards.

5.3.2.3 Recalling archived health data

Data that has been archived can be accessed via a request to the health data custodian or controller as guided by the Digital Health (Health Information Management Procedures) Regulations, 2025. This data can be used for secondary data use or to meet requirements as set out by the data requestor within the confines of Kenyan law.

5.3.3 Data Disposal

Data disposal—also referred to as data destruction—is the irreversible process of rendering health data unusable, unreadable, or inaccessible once it has reached the end of its retention period and is no longer needed for operational, legal, or archival purposes.

Disposal must be:

- Secure, ensuring no unauthorised recovery or misuse
- Documented, with audit trails
- Compliant with the Data Protection Act (2019), the Digital Health Act (2023) – Section 35, and this Framework

Key Principle:

Destruction must only occur when all retention, audit, and regulatory obligations have been fulfilled.

Disposal Requirements

Health data controllers and processors must:

1. Notify the data subject, or the data custodian, before destroying sensitive personal data
2. Prepare a summary abstract of the data for continuity of care (e.g., essential medical history)
3. Maintain a destruction log containing:
   - Date and time of destruction
   - Type of data destroyed
   - Destruction method used
   - Authorised personnel involved
   - Reason for destruction
4. A health data controller who intends to stop dealing with health data shall ensure that the digital health solution that the health data controller has been utilizing shall archive all health data in the possession of that health data controller in the County Health Data Bank.

Approved Destruction Methods

Medium	Recommended Methods
Paper records	Shredding, incineration, pulping
Digital records	Secure data wiping, degaussing, cryptographic erasure, physical drive destruction
Cloud storage	Verified deletion with provider certification, revocation of access, permanent purge

All destruction activities must comply with established Standard Operating Procedures (SOPs) issued by the Ministry of Health and the Digital Health Agency.

Compliance Reminder:

Improper destruction of health data is a breach of the Data Protection Act and may trigger penalties under Kenyan law.

5.4 Disclosure

Disclosure refers to the intentional release of health data or information to an authorised third party. This may occur for clinical coordination, legal compliance, research, or other lawful purposes. Unlike routine access or internal sharing, disclosure involves a deliberate transfer of information outside its originator or custodian.

All disclosures of health data must uphold the data protection pprinciples of privacy, confidentiality, and informed consent, and comply within line with various regulations: and procedures.

Core Principle:

Health data may only be disclosed where there is a lawful basis, a legitimate purpose, and appropriate safeguards are in place.

Governance of Health Data Disclosure

1. **Legal and Ethical Basis**
   - All disclosures must be authorised by law, by the data subject (via consent), or by a competent oversight body
   - Disclosure for care, surveillance, or research must comply with ethical standards and professional confidentiality obligations
2. **Oversight Responsibilities**
   - The Digital Health Agency provides stewardship over data privacy and confidentiality
   - A Privacy, Security, and Confidentiality Plan must be maintained and regularly

updated to reflect new risks or changes in technology

3. **Disclosure Controls**
   - Physical, logical, and administrative controls must be enforced to:
     - Prevent unauthorised use or leakage
     - Log and monitor all disclosures
     - Ensure that disclosed data is proportionate, relevant, and protected during transit

Permissible Purposes of Disclosure

Health data may be disclosed for:

- Clinical referrals and continuity of care
- Public health investigations and disease surveillance
- Statistical reporting and health sector performance reviews
- Court orders or legal proceedings
- Accredited health research (with ethical approval)

Note: Disclosure must not exceed the scope of the original consent or lawful basis—and must never compromise patient dignity or safety.

5.5 Data Migration or Transfer of Data

Data migration refers to the process of moving health data from one system, storage location, or format to another. It typically occurs when upgrading systems, consolidating databases, or transitioning to new platforms. Data transfer, on the other hand, involves moving data to external systems or jurisdictions for processing, sharing, or storage.

Data migration and transfer must be carried out in a secure, controlled, and transparent manner to ensure that the integrity, confidentiality, and privacy of health data are maintained throughout the process.

Key Considerations for Data Migration and Transfer:

1. **Data Integrity**
   - All data being migrated or transferred must be accurate, complete, and consistent across systems.
   - Data mapping must ensure that legacy data formats align with new systems or platforms.

2. **Compliance with Legal and Ethical Standards**
   - Data migration must comply with the Data Protection Act (2019), the Digital Health Act (2023), and the Health Data Governance Framework (HDGF).
   - Migration or transfer of sensitive personal data must undergo a Data Protection Impact Assessment (DPIA).

3. **Security and Privacy**
   - Data must be encrypted during transfer or migration, both in transit and at rest, using approved encryption standards.
   - Access controls must be enforced, ensuring that only authorised personnel can migrate or transfer data.
   - A complete audit trail must be maintained throughout the migration or transfer process to ensure accountability.

Step	Description
1. Assess Data Landscape	Understand existing data sources, formats, and quality. Identify and map data for migration/ transfer
2. Set Clear Objectives	Define the purpose of migration/ transfer (e.g., system upgrade, consolidation). Set goals for accuracy and complete-ness.
3. Data Mapping and Transformation	Link old data fields to new formats. Apply necessary transformations during migration/ transfer.
4. Choose Appropriate Tools	Select secure tools for efficient data transfer (batch processing, real-time streaming, etc.).
5. Test Thoroughly	Validate data accuracy and integrity. Perform parallel runs to ensure no data loss.
6. Ensure Security and Privacy	Encrypt sensitive data and comply with DPA and DHA regulations.
7. Communicate and Train	Inform stakeholders about the migration plan and train users on new systems.
8. Monitor Progress	Track the progress of migration/ transfer. Resolve issues as they arise.
9. Post-Migration Activities	Archive old data if needed. Update documentation and metadata.

Table 5: Steps for Successful Data Migration/ Transfer

Security Requirement:

The data migration process should comply with all security protocols and data protection standards to ensure no data leakage or loss during the process.

5.6 Reporting and Incident Management

Incident management in the context of health data refers to the identification, reporting, investigation, and resolution of any event that leads to unauthorised access, modification, disclosure, or destruction of health data. Effective incident management is essential to maintain data integrity, protect data subjects' rights, and ensure compliance with legal frameworks.

Health data controllers, processors, and custodians must have established policies and procedures in place to manage data incidents effectively. These procedures must ensure that incidents are promptly detected, adequately investigated, and resolved according to the Data Protection Act (2019) and the Digital Health Act (2023).

5.6.1 Identification and Detection

Organisations and entities handling health data must implement systems and processes that can detect potential data breaches or incidents. This includes:

- Intrusion detection systems (IDS) and access control logs to monitor unauthorised attempts to access health data.
- Regular system audits and checks for vulnerabilities in data handling and storage processes.
- Proactive risk assessments to identify and mitigate potential threats before they lead to incidents.

5.6.2 Investigation

Once an incident is identified, health data controllers and processors must:

1. Investigate the cause and scope of the incident.
2. Document the findings of the investigation, including any system weaknesses, procedural failures, or human errors that led to the incident.
3. Evaluate the potential impact on data subjects and the health data system, particularly with regard to PII or sensitive personal data.

Principle:

All investigations should be conducted transparently, and findings should be shared with relevant authorities and stakeholders, such as the Digital Health Agency and ODPC.

5.6.3 Resolution

After an investigation, the organisation must:

1. Mitigate the immediate impact of the incident—e.g., by shutting down compromised systems, notifying affected individuals, and containing any data leaks.
2. Implement corrective actions to prevent the recurrence of the incident. This may include:
   - Revising policies, procedures, and security measures
   - Introducing new training or awareness programs for staff
   - Upgrading technical controls (e.g., enhancing encryption or access restrictions)

5.6.4 Reporting to the Digital Health Agency and ODPC

In the event of a data breach or other incident, the affected organization or the data controller is required to:

- Notify the Digital Health Agency within 48-hours of identifying the health data breach (DHA, 2023) and within 72 hours of the notification of the breach to the DHA, provide a report detailing the
  - corrective measures taken;
  - mitigation actions adopted;
  - timelines for the rectification of the breach; and
  - in the case of sensitive personal data, any actions taken to assist data subjects whose data was involved in the breach.
- Notify the ODPC within 72 hours of discovering a data breach involving sensitive personal data (DPA, 2019)
- Notify other authorities based on procedures such as Data sharing Agreements
- Ensure all affected parties (including data subjects) are notified promptly and correctly, in accordance with data protection laws.

5.6.5 Risk Assessment & Mitigation

Routine risk and impact assessments must be conducted to assess vulnerabilities in the data handling processes. These assessments must:

1. Identify potential threats and weak points in the system.
2. Evaluate the likelihood and consequences of each risk.
3. Propose mitigation strategies and monitor their implementation.

Regular DPIAs:

These assessments should be conducted annually or when introducing new systems or processing methods that involve sensitive data.

All institutions must document their efforts to mitigate risks, as required under the DPA, 2019. Penalties for non-compliance are outlined in the Act and should be considered when planning and implementing risk mitigation measures.

5.7 Summary

This chapter has outlined the comprehensive processes involved in managing health data across its entire lifecycle—from data collection and processing to retention, disclosure, and destruction. Each phase of this lifecycle has been guided by strict principles of security, privacy, confidentiality, and data quality to ensure that health data is handled with the utmost care and responsibility.

Key points covered include:

- The importance of data quality and standardisation through initiatives like the National Health Data Dictionary (NHDD) and alignment with international best practices.
- The responsibilities of data controllers, processors, and other key actors to maintain legal and ethical standards throughout the data lifecycle.
- The role of the Digital Health Agency in overseeing the national health data infrastructure, ensuring interoperability, and promoting security and confidentiality.
- The processes for incident management, ensuring that health data breaches or risks are identified, investigated, and mitigated effectively.

As Kenya's health sector continues to digitalise, it is vital that these principles and processes be operationalised across the entire ecosystem. **Chapter 6** will focus on how these frameworks are implemented in practice, detailing the monitoring, evaluation, and continuous improvement mechanisms needed to ensure long-term success in health data governance.

6 Implementation Plan

This chapter outlines:

1. The key strategies and activities required to operationalise the Health Data Governance Framework (HDGF) in Kenya.
2. The short-, medium-, and long-term phases for implementing the framework.
3. The approach for engaging stakeholders to ensure active participation.

6.1 Introduction

The successful implementation of the Health Data Governance Framework (HDGF) is essential for realising Kenya's vision of an equitable, secure, and efficient health data system. Chapter 1 laid the groundwork by outlining the need for a centralised governance structure and strategic objectives that address health data governance challenges across the country. Chapters 2 to 5 then presented the regulatory landscape, governance principles, and data management processes needed to guide the application of the HDGF in Kenya's evolving health ecosystem.

This chapter translates those principles, roles, and responsibilities into actionable strategies and implementation phases. The objective of this Implementation Plan is to establish clear governance structures, facilitate stakeholder participation, and ensure the effective management of health data to improve care delivery, public health outcomes, and data-driven innovation.

The operationalisation of the HDGF must be systematic, encompassing:

- The creation and scaling of governance structures at various levels (national, county, facility)
- The development of tools, guidelines, and processes that make the governance framework actionable
- Capacity-building initiatives to support all stakeholders, from frontline healthcare workers to senior policymakers

This chapter will discuss the short, medium, and long-term strategies required to bring the HDGF to life, underpinned by a focus on transparency, data privacy, and stakeholder collaboration.

6.2 Key Implementation Phases

Phase 1: Establishment of Leadership and Governance (Short-Term: 2025-2026)

Governance Structures: The initial phase will focus on the establishment of key governance structures, as outlined in Chapter 4. This includes the Digital Health Agency (DHA) assuming its role as the Health Data Custodian and formalising its relationship with the Ministry of Health (MoH) and county health departments.

The **Digital Health TWG** will be set up to support the operationalisation of the Framework, while the Health Data Governance Coordination Mechanisms will be mapped out.

Key activities include:

- Formal launch of the HDGF and its supporting documents
- Appointment of leadership roles within governance structures
- Recruitment and capacity-building for roles such as data controllers, processors, and data protection officers (DPOs)
- National and County Health Data Banks establishment
- Initial awareness campaigns targeted at stakeholders from both state and non-state sectors

Context:

As described in **Chapter 1**, the HDGF seeks to improve transparency, privacy, and the effective use of health data. These initial governance structures are critical to ensuring the Framework's principles are respected from day one.

Phase 2: Engagement and Capacity Building (Medium-Term: 2027-2028)

Once the foundational structures are in place, the next step will involve deepening stakeholder engagement, capacity building, and developing the tools and processes necessary for implementing health data governance at scale.

Key activities include:

- Conducting training sessions for data controllers, processors, and relevant stakeholders at the national, county, and facility levels.
- Implementing tools like the National Health Data Dictionary (NHDD) and other data governance templates.
- Hosting the Health Data Sharing and Learning Forum, where stakeholders share best practices and discuss emerging challenges in data governance.
- Strengthening national reporting systems and ensuring compliance with the monitoring and evaluation (M&E) system outlined in Chapter 7.

This phase will be marked by a focus on collaboration, integration, and scaling. By engaging stakeholders from diverse sectors, Kenya will lay the groundwork for a sustainable digital health ecosystem.

Key Link:

This phase aligns with the institutional responsibilities discussed in Chapter 4, where we define roles and coordinating bodies like the Digital Health Agency and MoH.

Phase 3: Scaling and Monitoring (Long-Term: 2029-2030)

The final phase will focus on scaling the HDGF across the country, ensuring that systems and practices are implemented and monitored consistently. This phase will also involve continuous improvement and adaptation to new digital health challenges, ensuring the governance system remains robust and responsive.

Key activities include:

- Nationwide implementation of HDGF across all health facilities and counties, including full integration of digital health tools.
- Ongoing capacity strengthening and monitoring through the M&E framework outlined in Chapter 7.
- Periodic updates and revisions of the HDGF, informed by lessons learned, changing technologies, and evolving health data needs.

Iterative Improvement:

As described in Chapter 5, continuous monitoring, data quality assurance, and incident management will be essential to sustaining the integrity of health data governance in the long term.

6.3 Stakeholder Engagement

Successful implementation requires collaboration across multiple actors, including government entities, non-governmental organisations, health institutions, and the private sector. Stakeholders play distinct but complementary roles in the health data ecosystem, as outlined in Chapter 4.

Strategic engagement will include:

- Regular consultations and feedback loops with data subjects, county health departments, NGOs, and other partners.
- Public-private collaboration through targeted communication campaigns to raise awareness and build trust in the HDGF.
- Leveraging multi-stakeholder forums such as the Health Data Sharing and Learning Forum to refine data governance processes and tackle emerging issues.

Ongoing capacity building will be essential to keep stakeholders informed about new technologies, best practices, and data protection standards. This ensures that all actors involved can effectively contribute to health data governance and make informed decisions.

Inclusive Governance: Chapter 1 highlights the importance of inclusivity—this principle will be carried forward through continuous engagement with stakeholders from across Kenya's diverse health sectors.

6.4 Monitoring and Evaluation

Continuous monitoring and evaluation (M&E) are key to ensuring the success and sustainability of the HDGF. This will be operationalised through the M&E Framework described in Chapter 7. Key activities include:

- Tracking implementation progress and assessing the impact of the Framework on health outcomes, data quality, and privacy.
- Feedback loops for stakeholders to report on challenges and successes during periodic assessments.
- Iterative updates to the Framework to reflect evolving technologies, policies, and governance practices.

Dynamic M&E System:

The Chapter 7 M&E framework will ensure that the HDGF evolves with Kenya's digital health landscape, tracking real-time progress and making data-informed adjustments.

6.5 Summary

The Implementation Plan described in this chapter details the phased rollout of the Health Data Governance Framework (HDGF) in Kenya. With clear milestones for the short, medium, and long-term, and active stakeholder engagement, the HDGF will guide Kenya toward a more secure, equitable, and innovative health data ecosystem. Monitoring and evaluation mechanisms will ensure that progress is tracked, goals are met, and governance is sustained across the health sector.

7 Monitoring, Evaluation and Learning

This chapter outlines:

1. The monitoring, evaluation, and learning framework that will help determine the effectiveness of implementing the Health Data Governance Framework (HDGF).
2. The key information to be tracked, including roles, responsibilities, and resources required for effective monitoring and evaluation activities.
3. The approach for conducting learning activities to ensure continuous improvement and adaptive management of the health data governance process.

7.1 Introduction

This section outlines the monitoring, evaluation, and learning framework for the implementation of the Health Data Governance Framework (HDGF) in Kenya. It focuses on tracking the progress of the framework's implementation, evaluating its effectiveness, and identifying opportunities for continuous improvement. Monitoring and evaluation are critical for ensuring that the framework achieves its goals—enhancing data sharing, improving data quality, promoting equity, increasing data utilization, and safeguarding the privacy and security of health data.

The Health Data Governance Framework also serves as a platform for accountability and learning, enabling stakeholders to track progress, make evidence-based decisions, and optimize the health system's performance. Through regular reviews, the Ministry of Health (MoH) will collaborate with relevant stakeholders to ensure that the framework remains aligned with the evolving objectives of the health sector.

At the start of implementation, a baseline measurement will be conducted to establish a reference point for assessing the effectiveness of interventions over time. This baseline will inform target-setting, identify potential gaps, and provide insights into the initial challenges faced. Mid-term and end-term reviews will follow, offering valuable data on the framework's progress, impact, and areas for further improvement.

Table 6 below presents the HDGF implementation matrix, which outlines the scope of the monitoring, evaluation, and learning plan discussed in this chapter.

Key Activity	Sub-Activity	2025	2026	2027	2028	2029
Awareness and advocacy amongst stakeholders	Finalisation and Launch of the Health Data Governance Framework	X				
	Dissemination and sensitisation of stakeholders	X	X	X	X	X
Implementing Data Governance Framework	Formation of Data Governance Structures					
	Strategic	X	X	X	X	X
	Operational	X				
	Adaptation and operationalisation of Health Data Governance Tools across the health data management lifecycle	X	X	X	X	X
Monitoring, Evaluation and Learning	Monitoring	X	X	X	X	
	Evaluation	X	X	X	X	X
	Baseline/Formative Assessment	X				
	Mid-term Review			X		
	End-term Review					X
	Learning	X	X	X	X	X
	Health Data Governance Sharing and Learning Forum	X	X	X	X	X

Table 6: HDGF Implementation Matrix

As described in the implementation matrix above, three key reviews will be undertaken at baseline (year 1), mid-term (year 3), and end-term (year 3) to assess the progress and effectiveness of implementing the Framework.

The baseline review will be conducted before the implementation process begins to establish a starting point and provide a benchmark against which progress can be measured. The review will include an assessment of the current data governance practices and infrastructure in the country, as well as any existing policies, laws, and regulations related to health data. This review will help to identify the strengths, weaknesses, opportunities, and threats of the existing system, and inform the development of the health data governance Framework.

The mid-term review will be conducted approximately halfway through the implementation process. This review will assess the progress made in the implementation of the Framework, identify any challenges or obstacles encountered, and evaluate the effectiveness of the data governance structures and processes that have been established. This review will help to identify areas where improvements are needed and provide an opportunity to adjust the implementation plan.

The end-term review will be conducted at the end of the implementation process. This review will assess the overall impact of the Framework on healthcare outcomes, evaluate the effectiveness of the data governance structures and processes that have been established, and identify areas for further improvement. This review will provide the basis for and an opportunity to celebrate successes, identify best practices, and make recommendations for future improvements.

The baseline, mid-term, and end-term reviews will collectively evaluate the implementation process of the entire Framework. Their comprehensive assessment will assist in ensuring the success of the Framework, and in turn, improve the effectiveness of health service delivery and outcomes in Kenya. Table 7 below shows the indicator definition matrix that describes the key indicators that will be tracked during implementation of the HDGF.

Indicator	Description	Level	Data Source	Frequency
Number of indicators and data sets shared with regional and international partners	Indicates how many indicators and datasets are shared between Kenya and its global partners	National/County	Health Information Systems	Annual
Number of counties that have documented standard SOPs for data access, use, and sharing	Shows the number of counties with official SOPs for handling data access and sharing	County	County Health Offices	Annual
Number of employees trained on data protection	Tracks how many individuals working in the health sector have received training on data protec-tion	National/County	HR Records	Annual
Number of State and non-State actors complying with the Data Protection Regulations	Measures compliance with Data Protection regulations by both government and private entities	National/County	Compliance Report	Semi-Annual
Awareness of Data Protection among State and non-State actors	Reflects how aware State and non-State actors are regarding data protection principles	National/County	Surveys/ Interviews	Annual
Trust in the Health Sys-tems by Data Subjects	Indicates the level of trust patients and citizens have in the health data management systems	National	Surveys/ Feedback	Annual

Table 7: Indicator Definition Matrix

7.2 Monitoring and Enforcing Compliance

Entities and individuals entrusted with handling sensitive personal and health data must be fully aware of the legal requirements surrounding data protection. Ministries, agencies, and departments should implement measures to prevent unauthorized access or leakage of personal health data. These measures will include restricting data access to specific, stated purposes and assigning access permissions based on job roles and responsibilities.

Health data, including both general and personal information, must be treated as confidential. It is the responsibility of all staff and involved parties to preserve the confidentiality of any data they access. When sharing data with external affiliates, strict adherence to applicable laws, including the terms outlined in Data Use and Sharing Agreements and Non-Disclosure Agreements (NDAs), must be followed.

Any careless or malicious disclosure of data will be considered a legal liability for the individuals responsible for the data collection and processing.

Agencies and departments collecting and processing data hold intellectual property rights (IPR) in accordance with existing national and organizational laws. Any movement or transformation of data must be authorized in advance, following the governance structures outlined in Section 4 of this Framework.

This section also outlines recommended monitoring and assessment procedures, including the following checklist:

1. Ensure that regular audits of data processing activities and security controls are scheduled.
2. Maintain up-to-date records of personal data to facilitate efficient access, sharing, and use.
3. Conduct Data Protection Impact Audits (DPIAs) when required.
4. Regularly assess data protection practices and address compliance with the Data Protection Act.

Table 8 below presents the work plan for monitoring and evaluating the implementation of the Health Data Governance Framework.

GOAL: An adopted and implemeted Kenya Health Data Governance Framework														
Activity	Indicator	Target	Data Source Method/tool)	Output	Frequency of data collection	Responsible Person(s)	Purpose of indicator (Process outcome, Impact)	Baseline	Period of implementation (Year) 2024	2025	2026	2027	2028	2029	Comments
Advocate and create awareness on the KHDGF amongst stakeholders at the National level and in the 47 counties	Number of launch and dissemination meetings held	4 dissemination forums	1. launch and dissemination meeting report 2. participants list	National MoH, DHA, 47 counties and other Health stakeholders sensitized, and awareness created on KHDGF	Biannual	Head Division of Policy and Research	Process		X	X					This will be 4 forums held either virtually or in person to disseminate the DGF to stakeholders at all levels. 2 forums on each half of the year.
	Number/ proportion of counties that have held dissermination forums with facility staff	47 counties	1. Meeting report per county		Biannual	County data governance focal person	Process		X	X					This will be county driven forums to disseminate he DGF to stakeholders within the county and is an ongoing process depending on funds availability
Establish and support the implementation of data governance framework	Number/ proportion of counties with updated data governance tools/SOPs	47 counties	1. Distribution list 2. Technical assistance counties report	Guidelines, Policies and SOPs on data governance are adopted by Data Controllers and Processors	Annual	Head Division of Policy and Research	Outcome			X	X X	X X	X X	X X	
	Number/ proportion of counties with data governance structures in place at county level	47 counties	1. Documented county level governance structure including identification of a data governance focal person 2. Meeting minutes which include data governance as an agenda		Annual	County data governance TWG chairperson	Outcome			X	X	X	X	X	To be initiated after dissemination of the DGF by the national level and counties will be left to appoint the focal person and also initiate data governance in their forums
	Number of technical assistance missions on KHDGF conducted	2				National data governance TWG chairperson	Output								To be conducted at all levels. A tool will be developed to aid in monitoring uptake of data governance issues as documented in the framework
Monitore and evaluate of the KHDGF implementation	Number of baseline survey conducted	1 baseline survey	Baseline survey report	Disseminated M&E reports on KHDGF implemetation progress	Annual	Head Division of Policy and Research	Impact		X						To be conducted in the first year to determine the level of data
	Number of Midterm evaluation of the DGF conducted	1 mid term survey	Mid term survey report		Annual		Impact				X				To be conducted in the first 3 years to monitor uptake of the DGF at all levels of health care delivery
	Number of end term evaluation of the DGF conducted	1 end term survey	End term survey report		Annual		Impact						X		To be conducted towards the end of the life cycle of the document to inform the future

Table 8: Workplan for Monitoring and Evaluation

ANNEX 1: LIST OF CONTRIBUTORS

Reviewers

Ministry of Health

Dr. Zeinab Gura
Dr. David Soti
Dr. Denver Mariga
Dr. Nancy Njeru

Editors

Ministry of Health	Palladium	Tony Blair Institute	University of Washington
Dr. Joyce Wamicwe	Pascal Mwele	Dr. Ramona Koech	George Owiso
Waigumo G. Kiragu	Dr. Jacob Odhiambo	Steve Wanyee - Consultant	
	Evans Munene		

Contributors

Ministry of Health		Partners	
Dr. Ayub Manya	Susan Kihiu	Adan Muhamed	Peter Yegon
Dr. Bernard Langat	Daniel Mumbia	Ann Muiruri	Phillip Muchiri
Beatrice Oyoo	Dr. Joseph Sitienei	Dr. Bashir Ahmed	Rachel Wanjiru
Catherine Matioli	Dr. Hellen Kiarie	Dr. Beatrice Kariuki	Raphael Ondondo
Esther Kathini	Nicholas Macharia	Dr. Calvine Lwaka	Raphael Pundo
Elvis Muriithi		Christopher Komen	Dr. Reuben Thuo
Faith Ngari	**MoICDE**	Dr. David Kariuki	Rose Kirinya
Francis Nyamari	Eric Nderitu	Diana Too	Rose Nzioka
Galmo Dulacha	Justin Mbogo	Edwin Syeunda	Shalin Moraa
Hellen Masila		Dr. Eric Mbuthia	Prof. Simon Karanja
Dr. Jeremiah Mumo	**Ministry of Defense**	Francis Njiri	Dr. Sylvia Mwelu
Dr. Job Nyangena	Col. Edward Mutinda	Prof. Fred Wamunyokoli	Timothy Wafula
Dr. Joseph Sitienei		Jachen Schmidt	Victor Were
Dr. Martha Muthami	**Counties & COG Secretariat**	Joseph Mugah	Wilson Mbogo
Michael Mwangi	Elizabeth Oele	Dr. Josephine Nguri	
Onesmus Kamau	Dr. Gregory Ganda	Dr. Kamau Mwangi	**Design**
Paul Malusi	Michael Kibiwot	Dr. Kennedy Muthoka	Brian Ogutu
Rono Cherotich	Dr. Papela Wanjala	Dr. Kigathi Wanjru	
Dr. Ryan Nyotu	Dr. Paul Musila	Margaret Ndisha	
Stella Wanja	Mebor Abuor	Martha Ogutu	
Steve Mutua		Maureen Adoyo	
Dr. Wesley Ooga	**Statehouse Kenya - Policy**	Muchemi Wambugu	
Annette Omwoyo	Corrine Bore	Dr. Nelly Nyaga	
Terry Rotich		Nelson Otuoma	
Bernard Kuria	**ODPC**	Pauline Omoto	
Olivia Simitu	Rose Mosero	Peter Muya	
Lily Samich	Diana Ilako	Prof. Peter W. Wagacha	
Paul Wekesa			

***MoICDE** ~ Ministry of ICT and the Digital Economy
***ODPC** ~ Office of the Data Protection Commissioner

MINISTRY OF HEALTH

AFYA HOUSE, CATHEDRAL ROAD
P.O. BOX: 30016 - 00100, NAIROBI
www.health.go.ke