REPUBLIC OF KENYA

MINISTRY OF HEALTH

DIGITAL HEALTH SOLUTIONS STANDARDS AND GUIDELINES

2025

MINISTRY OF HEALTH

DIGITAL HEALTH SOLUTIONS STANDARDS AND GUIDELINES 2025

Suggested caitation: Ministry of Health, Kenya. Digital Health Solutions Standards and Guidelines 2025

Ministry of Health
P.O. Box 30016-00100
Nairobi, Kenya.
Website: https://www.health.go.ke/

Table of Contents

Foreword

Kenya's health system stands at a critical juncture—where the urgency to improve health outcomes intersects with the transformative power of digital innovation. As we work toward achieving universal health coverage and strengthening our health system's resilience, the need for coordinated, standards-based digital health solutions has never been greater.

Anchored in the Digital Health Act, 2023, the Digital Health Standards and guidelines represent a bold step forward in Kenya's digital health journey and in the implementation of the Kenya Health Enterprise Architecture. This clearly demonstrates our shared vision for a resilient, secure, and connected, digital health ecosystem, collaborative and consultative process, these standards are designed to provide clear, practical direction to developers, implementers, and health sector stakeholders. They offer a blueprint for designing and deploying digital health tools that are not only technically sound but also responsive to the real needs of patients, providers, and communities.

We recognize that digital health is not simply about technology—it is about systems working better for people. These guidelines address key elements such as system architecture, data standards, user experience, interoperability, and sustainability. They ensure that digital health investments are built on a foundation of quality, scalability, and equity.

As a government, we are determined to create an environment that nurtures innovation while safeguarding patient rights, data privacy, and clinical safety. This document is a critical instrument to align the growing digital health ecosystem with national health priorities and global best practices.

I commend all stakeholders who contributed to this important work, and I call upon all public and private sector actors to adopt and apply these standards. Let us work together to build a cohesive digital health landscape that delivers meaningful impact for all Kenyans.

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

Preface

The Kenya Digital Health Standards and Guidelines represent a pivotal step in transforming healthcare delivery across the country. By consolidating frameworks informed by global best practices—such as ISO, FHIR, and NIST—and aligned with Kenya's legislative and policy landscape, including the Data Protection Act (2019) and the Digital Health Act (2023), this document provides an enabling foundation for implementing secure, interoperable, and efficient digital health solutions.

As the adoption of digital technologies in healthcare expands, uncoordinated implementation has historically resulted in fragmented systems, data silos, and inefficiencies. These standards and guidelines are designed to address such challenges by defining functional requirements for systems, specifying minimum data sets for interoperability, and ensuring adherence to privacy and security principles. This strategic approach aims to enable seamless exchange of patient data, enhance decisionmaking, and improve healthcare outcomes.

Kenya's journey in digital health has seen remarkable milestones, from early disease-specific systems to integrated solutions spanning diverse healthcare domains. These achievements have been made possible through the collective efforts of stakeholders, including government agencies, implementing partners, and health informatics experts. The enactment of the Digital Health Act (2023) further underscores the government's commitment to advancing digital health through the establishment of the Digital Health Agency (DHA). The DHA is mandated to oversee the creation of a comprehensive, integrated digital health information system, empowering continuity of care at all levels of healthcare.

This document outlines guidelines for system developers and implementers, emphasizing the need for interoperability, data quality, and security. By referencing international standards and local regulations, it provides a consistent framework for stakeholders to follow, ensuring data integrity, protecting patient privacy, and safeguarding healthcare systems from potential vulnerabilities. The Ministry of Health acknowledges the transformative potential of Information and Communication Technology (ICT) in improving service delivery, promoting equity in healthcare access, and enhancing the governance of health information systems. It is through adherence to these standards that Kenya can build a resilient, efficient, and accessible healthcare system. This publication has been developed through an iterative and participatory process, engaging government agencies, development partners, patient groups, and other stakeholders. It reflects a shared vision of delivering high-quality, accessible healthcare services to all Kenyans. The Ministry of Health remains committed to reviewing and updating these guidelines regularly to ensure they remain relevant to technological advancements and evolving healthcare needs. By embracing these standards, stakeholders contribute to delivering high-quality, accessible healthcare for all Kenyans.

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

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

Acknowledgement

The Ministry of Health (MoH) extends its deepest gratitude to all organizations, experts, and stakeholders whose contributions have been instrumental in the development of these digital health standards and guidelines.

We acknowledge the invaluable strategic leadership and guidance provided by Hon. Aden Duale, EGH, Cabinet Secretary for Health, whose stewardship has ensured the alignment of these guidelines with Kenya's health priorities and strategic goals.

This document is a product of an iterative and consultative process that involved extensive engagement with diverse stakeholders, including patient groups, development partners, and health sector professionals. Their insights and feedback were pivotal in shaping a document that is both comprehensive and practical for implementation.

Our heartfelt thanks go to the MoH Directorate of Health Financing, Digital Health Policy and Research, and the Digital Health Agency for their unwavering commitment and technical expertise throughout the development process. Special thanks to Dr. Ayub Manya, Dr. Wesley Ooga and Dr. Jeremiah Mumo, all from the MoH, for seeing through the development of this framework. We also extend special thanks to the Ministry of Information, Communications, and the Digital Economy for their vital contributions to ensuring the alignment of ICT frameworks with the health sector's needs.

Our gratitude extends to the funding and technical support provided by the U.S. Centers for Disease Control and Prevention (CDC) through a cooperative agreement with the University of Washington's International Training and Education Center for Health (I-TECH) and Palladium.

We also wish to recognize the contributions of WHO, USAID, Intellisoft, HELINA, PATH, the University of Nairobi (Health IT and TAP Projects), Savanna Informatics, Medtronics, and DARP. Their collaborative efforts have enriched the quality and scope of this document.

Lastly, we thank all individuals and institutions whose commitment to advancing Kenya's digital health ecosystem has made this publication possible. Your efforts ensure that the Kenyan health sector continues to thrive in the digital age, improving healthcare delivery and outcomes for all.

Dr. Patrick O. Amoth, CBS
Director General for Health,
Ministry of Health

Executive Summary

The Kenyan healthcare system is undergoing a digital transformation to enhance efficiency, interoperability, and access to quality care. This publication consolidates key standards and guidelines essential for implementing secure, efficient, and interoperable digital health solutions across the country. It serves as a comprehensive framework for digital solution developers, healthcare implementers, policymakers, and other stakeholders, guiding the adoption of digital health technologies that align with Kenya's regulatory framework, the Kenya Health Enterprise Architecture, and International best practices.

Objectives of the Standards and Guidelines

The primary objective of these standards is to provide a unified approach to designing, implementing, and maintaining digital health systems. By standardizing digital health solutions, this document aims to:

- **Promote Interoperability:** Facilitate seamless data exchange between systems using globally recognized standards such as FHIR, HL7, and ISO Health Informatics.
- **Enhance Security and Privacy:** Ensure patient data is protected in accordance with the Data Protection Act (2019) and other international standards like NIST.
- **Support Decision-Making:** Enable accurate and timely reporting, analytics, and clinical decision-making through standardized data management.
- **Ensure System Sustainability:** Provide guidelines for scalable and future-proof ICT infrastructure and systems.

Key Components of the Standards

1. **Community Health Solutions:**
    - Focused on demographic data capture, clinical decision support, reporting, and health information exchange
    - Emphasizes scalability, usability, and compliance with national health goals.
2. **Facility-Level Systems:**
    - Includes Electronic Medical Records (EMR), Laboratory Information Systems (LIS), Pharmacy Information Systems (PIS), and more.
    - Details functional requirements such as patient registration, inventory management, billing, and data security.
3. **ICT Infrastructure and Governance:**
    - Establishes standards for ICT equipment, network systems, cloud computing, and data centers.
    - Promotes sustainability, efficiency, and compliance with the Digital Health Act (2023).
4. **Security, Privacy, and Confidentiality:**
    - Implements robust access controls, data encryption, and incident response plans to protect sensitive health data
    - Aligns with global frameworks such as the NIST Cybersecurity Framework.
5. **Data Protection and Governance:**
    - Provides a framework for secure data collection, storage, and exchange in compliance with Kenyan laws and global best practices.
    - Reinforces accountability through regular audits, risk assessments, and compliance monitoring.
6. **Logistics and Supply Chain Management:**
    - Integrates standards for forecasting, procurement, and inventory management of health commodities.
    - Enhances efficiency in logistics management to support healthcare delivery.

Strategic Benefits

These guidelines are critical to advancing Kenya's health sector by addressing current challenges such as fragmented systems, limited interoperability, and security vulnerabilities. The benefits include:

- **Improved Service Delivery:** Streamlined workflows and decision support systems for healthcare providers.
- **Data-Driven Decision-Making:** Access to real-time data for policy formulation and resource allocation.
- **Strengthened Trust:** Enhanced confidence among patients and stakeholders through secure and reliable health systems.
- **Global Competitiveness:** Alignment with international health informatics standards fosters innovation and collaboration.

Audience and Applicability

The publication targets a wide range of stakeholders, including:

- **Developers and Implementers:** To ensure systems meet functional and technical requirements.
- **Government Agencies:** To guide national and county-level ICT planning and execution.
- **Policy Makers:** To align strategies with the standards and foster coordinated digital health adoption.
- **Donors and Development Partners:** To support investments in scalable and sustainable digital health solutions.

Call to Action

The Ministry of Health encourages all stakeholders to adopt and integrate these standards into their operations. By doing so, Kenya will accelerate its journey toward achieving universal health coverage, improving healthcare outcomes, and building a resilient digital health ecosystem.

Acronyms

ADR	Adverse Drug Reaction
AIDS	Acquired Immunodeficiency Syndrome
API	Application Programming Interface
ART	Antiretroviral Therapy
BMI	Body Mass Index
BSA	Body Surface Area
CDA	Clinical Document Architecture
CHU	Community Health Unit
CR	Client Registry
CSD	Care Services Discovery
DHA	Digital Health Agency
DHIS	District Health Information System
DLP	Data Loss Prevention
EHR	Electronic Health Record
EMR	Electronic Medical Record
FHIR	Fast Healthcare Interoperability Resources
FR	Facility Registry
GIS	Geographic Information System
HIE	Health Information Exchange
HIMSS	Healthcare Information and Management Systems Society
HIS	Division of Health Information Systems
HIV	Human Immunodeficiency Virus
HR	Human Resources
ICD10	International Classification of Diseases 10th Revision
ICT	Information and Communication Technology
ICTA	Information and Communication Technology Authority
IT	Information Technology
JSON	JavaScript Object Notation
KHEA	Kenya Health Enterprise Architecture
KMHFR	Kenya Master Health Facility Registry
LD	Laboratory Device
LIS	Laboratory Information System
LMIS	Laboratory Management Information System
LOINC	Logical Observation Identifiers Names and Codes
MFA	Multi-factor authentication
MICDE	Ministry of Information, Communications and The Digital Economy
MoH	Ministry of Health
MUAC	Mid Upper Arm Circumference
NEMA	National Environmental Management Authority
NIST	National Institute of Standards and Technology
OHIE	Open Health Information Exchange
OI	Opportunistic Infection
OS	Operating System
PR	ProviderRegistry
SHR	Shared Health Record
SNOMED	Systematized Medical Nomenclature for Medicine–Clinical Terminology
SOP	Standard Operating Procedure
TB	Tuberculosis

TCP/IP	Transmission Control Protocol/Internet Protocol
UPS	Uninterruptible Power Supply
XML	Extensible Markup Language
mCSD	Mobile Care Services Discovery

Definition of Terms

TERM	DEFINITION
Accession	Receipt, sorting and unique identification of a specimen in the laboratory.
Aliquot	A portion of the whole, especially one of two or more samples of something that have the same volume or weight.
Centrifugation	A process used to separate or concentrate materials suspended in a liquid medium.
Functional Profile	Selected set of functions that are applicable for a particular purpose, user, care setting, domain, etcetera.
EMR	A computerized legal medical record created by organizations 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.
eHealth	Healthcare services which are supported by digital processes, communication or technology such as electronic prescribing, Telehealth, or Electronic Health Records.
Architecture	Components such as electronic medical records systems, laboratory information systems, monitoring and evaluation systems, and other HIS components, the technologies upon which those components depend on, the data formats used to exchange information between the components, and the circumstances of that information exchange.
Enterprise Architecture	A rigorous description of the structure of an enterprise, its breakdown into subsystems, the relationships between the subsystems, the relationships with the external environment, the terminology in use, and the guiding principles for the design and evolution of an enterprise.
FHIR Standard	Fast Healthcare Interoperability Resources standard defines how healthcare information can be exchanged between different computer systems regardless of how it is stored in those systems. It allows healthcare information, including clinical and administrative data, to be available securely to those who have a need to access it, and to those who have the right to do so for the benefit of a patient receiving care.
Privacy	A legal concept referring to the protection accorded to an individual to control access to and use of personal information. Privacy protections vary from one jurisdiction to another and are defined by laws.
Confidentiality	Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
Security	The process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorized access.
Proficiency testing	The use of inter-laboratory study to determine the performance of individual laboratories for specific tests and to monitor laboratories' continuing performance (ISO/IEC 17025). (current 27001)

1.0 Introduction

Globally, several organizations have developed standards around medical information exchange, medical terminologies, and electronic health record systems functionalities. Additional standards have covered areas around the security of health information systems. Among the standards available for electronic health systems are ISO
standards, FHIR standards, International Classification of Diseases (ICD-11), LOINC and SNOMED.

In Kenya, the Kenya Bureau of Standards holds the mandate for adopting best practices and developing standards that regulate various industries and sectors. However, the implementation and enforcement of the developed standards lie within the purview of the relevant stakeholders including ministries such as the Ministry of Health.

In line with its commitment to fostering standardization and enhancing quality, KEBS has progressed the adoption and domestication of ISO Health Informatics Standards developed by ISO TC 215. This proactive approach aims to align Kenya's healthcare system with internationally recognized standards, ensuring interoperability, efficiency, and quality in health informatics practices across the country.

The Digital Health Standards and Guidelines significantly incorporate and build upon the standards developed and recognized by KEBS. They seek to provide concise, hands-on, implementable resources for groups implementing digital health solutions.

The following international standards will be referenced in this document:

Reference	Category	Scope
ISO 22220	Health Informatics	Identification of subjects of health care
TR 20514	Health Informatics	Electronic health record definition, scope and context
ISO 13606	Health Informatics	Health informatics electronic health record communication Parts 1,2,3 and 4 Part I of ISO 13606 specifies the information architecture required for interoperable communications between systems and services that need or provide EHR data Part II of ISO 13606 specifies the communication of part or all the electronic health record (EHR) of a single identified subject of care between EHR systems, or between EHR systems and a centralized EHR data repository
ISO/TR 18307:2001	Health Informatics	Interoperability and compatibility in messaging and communication standards key characteristics
ISO/TS 18308:2004	Health Informatics	Requirements for an electronic health record architecture

ISO 27799	Health Informatics	Health informatics, information security management in health using ISO/IEC 27002 This International Standard specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing this International Standard, health care organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organizations circumstances and that will maintain the confidentiality, integrity and availability of personal health information
ISO 17090:2008	Health Informatics	Public key infrastructure Parts 1, 2 and 3
HL7 FHIR	Health Information Exchange	A set of rules and specifications for exchanging electronic health care data

The Ministry of Health (MoH) has continually provided guidance in the development and adoption of digital health to support the provision of healthcare, through provision of digital health standards and guidelines. This has been an iterative process with revision conducted at regular intervals to address the changes in the digital health space over time. The last iteration of revising the standards and guidelines took place between 2013 and 2017. The output from the process was the realization of standards and guidelines for Primary Health Care (PHC), Pharmacy Information Systems (PIS), Laboratory Information Systems (LIS), mobile health (mhealth) and Health Information and Communication Technology (ICT) domains.

In an effort to ensure that the developed standards and guidelines remain relevant and aligned to the Kenya Health Enterprise Architecture, the MoH, supported by its implementing partners, embarked on a new iteration to review and update the existing documents. This document defines the minimum functional requirements for point of care systems adopted in Kenya, including community health systems, facility level systems, and logistics management information systems.

The objective is to ensure that every system developed in this space, provides the critical patient information to support continuity of care.

This document provides guidelines for the following range of systems:

1. Point of Care Systems
    a. Community Health Systems
    b. Facility Level Systems
        i. Electronic Medical Records (EMR) systems
        ii. Laboratory Information Systems (LIS)
        iii. Pharmacy Information Systems (PIS)
        iv. Medical Imaging systems

2. Logistics Management Information Systems (LMIS)

This document is intended for the following audiences:

a. Developers of digital health solutions for the Kenyan market.
b. Health systems or facilities currently using digital health systems.
c. Health systems or facilities considering procuring, adapting, or installing digital health systems or solutions, including public, private, mission, and NGO-supported facilities.
d. Health policy makers at all levels.
e. Development partners providing resources to support the Kenyan health system.
f. Regulatory and oversight bodies involved in accreditation, inspection, and compliance of digital health systems within the health sector

2.0 Functional Requirements

This section defines the minimum functional requirements that different digital health solutions are expected to meet.

2.1 Community Health Digital Solutions

Different community health digital systems can be developed for different purposes and health settings, and therefore, may have distinct functions and capabilities. Community Health Digital systems range from client care systems to integrated commodity management. To maintain a core set of functions and encourage best practices, this section details the recommended functional requirements for community health digital solutions including recommended capabilities that are categorized into the following 7 classes:

2.1.1 Basic demographic data

The system should align to the generic patient demographic data capture for unique client/patient identification. This includes:

1. Provide a unique patient ID
2. Create a patient profile
3. Modify a patient profile
4. Archive a patient profile
5. Search for a patient profile
6. Check for duplicates

2.1.2 Clinical decisions support

This refers to functions and processes that will assist health workers and clients in making clinical decisions. To support decision-making in clinical practice, systems are required to:

1. Alert the provider about abnormal (outside the normal range) vital signs.
2. Alert the provider about whether a known allergic drug is prescribed or if a known drug interaction is likely to occur.
3. Provide notification of recommended care and treatment.
4. Support diagnostic and analytic functions.
5. Provide reminders for preventive care and follow-up actions.

2.1.3 Health information and reporting

To improve quality of service, community health digital systems should improve and promote the use of health information amongst users. They should:

1. Generate reports from client data.
2. Generate aggregate data in a standardized format for use at all levels.

2.1.4 Health Information Exchange (HIE)

Health Information Exchange (HIE) is a system that allows healthcare professionals and patients to securely share vital medical information electronically. Community health digital systems should:

1. Be able to output and consume FHIR formatted patient data.
2. Integrate with the MoH electronic registries.

2.1.5 Audit trails

The system must log all system transactions. The records should include at least the following:

1. Date and time of the event
2. User ID or name
3. Type of event and the success or failure of that event

2.1.6 User Management

All the digital health solutions should:

1. Provide roles-based access
2. Require a unique user ID and password for system access
3. Allow authorized users to create, search, modify, delete user profiles

2.1.7 Information Security

The system should support the following functionality:

1. Log all login attempts
2. Provide timestamps for all transactions
3. Support data encryption at rest and in transit

2.1.8 Non-Functional Requirements

Community digital health solutions should at a minimum support the following nonfunctional requirements including:

1. Scalability
    a. Support easy addition of new modules
    b. Maintain acceptable response times with growing data
2. Usability
    a. Be intuitive to users interacting with the system.
3. Data validation
    a. Support control for allowable value ranges
    b. Enforce defined data formats

2.2 Facility-level Digital Health Solutions

As the number of systems implemented at the health facility continue to grow in this digital age, development of relevant guidelines aim to ensure that they meet the minimum requirements for supporting health care provision, health information exchange, and preservation of the integrity of the data collected through the systems.

It is desirable to maintain a core set of functions in each digital health solution at the facility level to support similar workflows and encourage best practices in clinical care. This section details the functional requirements, including required and recommended capabilities.

2.2.1 Registration

The system should align to the generic patient demographic data capture for unique client/patient identification. This includes:

1. Provide a unique patient ID
2. Create a patient profile
3. Modify a patient profile
4. Archive a patient profile
5. Search for a patient profile
6. Check for duplicates.
7. Merge duplicate patient profiles
8. Deactivate or retire a patient profile

2.2.2 Pharmacy and pharmaceutical products support

The system should:

1. Interoperate with the health products and technologies registry (HPTR).
2. Have prescription Management capabilities.
3. Manage pharmaceutical and non-pharmaceutical commodities management from HPTR on a store and dispensary Level (Inventory management).

2.2.3 Client record management

The system should:

1. Integrate with the Kenya National Health Terminologies Service1 (KNHTS) database to enable clinicians to pick diagnosis lists directly from them.
2. Capture triage information for both routine and emergency clients. At minimum, the system collects height, weight, pulse rate, respiratory rate, blood pressure, BMI (calculated), and MUAC for children.
3. Offer Lab services. Clinicians should be able to send requests to the lab and get results from the lab.
4. Support clinical decisions based on clinical guidelines.
5. Avail patient history including risk factors in cases of revisit.
6. Support clinical documentation/note taking capabilities.
7. Provide Appointment scheduling, notifications/reminders to users and clients

[1] https://knhts.health.go.ke/

2.2.4 Surveillance support management

The system should:

1. Monitoring of notifiable diseases and conditions.
2. Map and monitor thresholds for notifiable diseases with timely notification when thresholds are exceeded
3. Recommended public health actions for identified conditions.
4. Support query for notifiable or specific medical conditions, symptoms or diagnosis.
5. Have capability for contact identification and follow up.
6. Support disease specific data collection forms.

2.2.5 Reporting and analytics

The system should:

1. Support generation of standard MoH reports.
2. Support data visualization for service providers.

2.2.6 Laboratory and Diagnostics support

The system should support:

1. Order management (Create order/tests, receive orders, schedule orders, prioritize orders).
2. Sample management.
3. Laboratory Quality Assurance.
4. Equipment management.
5. Track consumables/reagents and commodities stock levels

2.2.7 Billing

The system should:

1. Generate and manage patient bills and invoices based on services rendered, procedures performed, medications prescribed, and other billable items.
2. Calculate costs, deductibles, copayments, and insurance coverage to determine patient balances and billing amounts.
3. Ability to configure and manage fee schedules, pricing structures, and reimbursement rates based on insurance plans, government programs, or self-pay arrangements.
4. Verify patient insurance eligibility, coverage details, and pre-authorization requirements before submitting claims.
5. Submit electronic insurance claims to payers (e.g. insurance companies, Social Health Insurance Fund (SHIF)) for reimbursement of healthcare services.
6. Comply with Electronic Data Interchange (EDI) standards for electronic claim submission.
7. Give a final diagnosis as per latest ICD.
8. Capture supporting documents to the claims being submitted, where needed. e.g., inpatient discharge summary and medical reports.
9. Identify, analyze, and resolve denied insurance claims by addressing coding errors, documentation deficiencies, and payer requirements.
10. Generating aging reports to track unpaid claims, outstanding balances, and accounts receivable (AR) aging trends for follow-up and collection activities.

11. Provide financial analytics and reporting capabilities to assess revenue trends, reimbursement rates, claim rejection rates, and overall revenue cycle performance.
12. Evaluate completion checks during claim submission to ensure nothing is missing from the claim.
13. Support addition of payers, with setup of price lists and tariffs.

2.2.8 Consents, Authorizations, and Directive

The system should:

1. Sign consent electronically or store a scanned manually signed consent form.
2. Create, maintain, and verify patient treatment decisions in the form of consents and authorizations when required.

2.2.9 Health Information Exchange (HIE)

The systems should:

1. Be able to output and consume FHIR formatted patient data.
2. Integrate with the MoH electronic registries.

2.2.10 Audit trails

The system must log all system transactions. The records should include at least the following:

1. Date and time of the event
2. User ID or name
3. Type of event and the success or failure of that event

2.2.11 User Management

All the digital health solutions should:

1. Provide roles-based access
2. Require a unique user ID and password for system access
3. Allow authorized users to create, search, modify, delete user profiles

2.2.12 Information Security

The system should support the following functionality:

1. Log all login attempts
2. Provide timestamps for all transactions
3. Support data encryption at rest and in transit

2.2.13 Non-Functional Requirement

The system should:

1. Maintain comprehensive technical documentation and user guide.

2. Have support for mediators.
3. Maintain user friendly interface.
4. Have capacity to grow with the health facility needs.
5. Support capture or upload of retrospective data.
6. Be easy to install, configure and maintain.

2. 3 Laboratory Information Systems

Medical laboratories are critical contributors to the health care system. They add valuable support to patient care through screening, diagnosis, follow-up, and promoting the treatment and prevention of disease. To facilitate these activities, medical laboratories rely on information systems. The two definitions of these information systems are as follows:

1. *Laboratory information systems* (LIS) are systems, usually computer-assisted, designed to store, manipulate, and retrieve information for management of administrative and clinical activities associated with the provision and utilization of clinical laboratory services. LIS provides a database that serves the information needs of the laboratory by linking patient test results to the ordering clinician/client and to the patient's medical record.
2. *Laboratory information management systems* (LIMS) are database applications that store and manage information associated with the laboratory, such as customers, sample matrices, tests, results, methods, parameters, employees, control limits, passwords, etc.

The terms LIS and LIMS are often used interchangeably because of the similarities between their definitions. We will use the term LIS in this document when referring to the electronic LIS. LIS has components that manage provider information, patient demographics, specimen accession and processing, results entry, and reporting.

The LIS standards and guidelines are guided by the following:

1. Laboratory guidelines from:
   a. Kenya's National Public Health Laboratory Services
   b. Association of Public Health Laboratories
   c. World Health Organization.
4. The Kenya HIS strategic plan and policy
5. Experience from MoH and partners in Kenya and from other countries
6. Published medical, laboratory, and public health literature.
7. Kenyan and international health informatics standards, including the International Organization for Standardization

This section details the functional requirements, including required and recommended capabilities.

2.3.1 User management

The systems should:

1. Provide roles-based access
2. Require a unique user ID and password for system access
3. Allow authorized users to create, search, modify, delete user profiles

2.3.2 Patient Management

The system should align to the generic patient demographic data capture for unique client/ patient identification. This includes:

1. Provide a unique patient ID
2. Create a patient profile
3. Modify a patient profile
4. Delete a patient profile
5. Search for a patient profile
6. Check for duplicates.
7. Merge duplicate patient profiles
8. Deactivate or retire a patient profile

2.3.3 Order management

A laboratory order is a request for laboratory testing. LIS should manage laboratory orders, including monitoring each order's status throughout the testing process. LIS should support universal laboratory order codes. Essential order management functions are:

1. Accept a new laboratory order request
2. Uniquely identify a laboratory order request
3. Prioritize laboratory requests
4. Accept patient information for received requests
5. Associate laboratory requests with specific patient information
6. Accept clinician information
7. Accept list of tests to be performed
8. Accept the specimen type
9. Accept the test procedure to be performed
10. Search for an order
11. Check for duplicate orders
12. Accept the facility name MFL code

The system shall support test scheduling. The LIS shall facilitate:

1. Unique identification of all the tests
2. Maintain a list of activities, tasks or events of the test process
3. Identification of the intended start and finish dates and/or times for the tests
4. Association of related test requests
5. Assignment of test equipment for specific tests
6. Scheduling of tests based on specific facility priority scales set during order entry on the LIS
7. Assignment of specific tests to particular laboratory technicians

The system shall support test scheduling. The LIS should have the ability to record the following:

1. The volume of each aliquot
2. The test kit number
3. The test instrument unique identifier
4. All the test data successful or failed tests
5. Allow tester to add comment on results that have not been sufficiently captured by predefined responses and any other relevant comment

6. Indicate tester's details i.e., name, contact and signature

2.3.4 Specimen management

Specimen management refers to the policies, procedures and infrastructure adopted to support the safe collection, handling and treatment and transport of biological specimens. (Cite integrated specimen referral guideline on Record keeping – WHO – Laboratory Quality Standard and Their Implementation: 2011) Essential specimen management functions for an LIS are:

2.3.4.1 Specimen Registration

The LIS should:

1. Generate unique specimen accession numbers that are linked to the original specimen ID
2. Generate labels for specimen containers, including barcodes and patient identifiers
3. Allow for batch registration of specimens
4. Accept scanned barcodes of specimen containers
5. Accept the date/time of specimen collection
6. Accept the date/time of specimen registration
7. Indicate the acceptance/rejection of specimens based on predefined criteria
8. Uniquely identify quality control specimens
9. Uniquely identify purpose for test analysis e.g., outbreak, emergency, travel, pr surveillance

2.3.4.2 Specimen Tracking

The LIS should provide a trail of specimen/sample custodians from the point of receipt until the disposal or return of results to the order requester

2.3.4.3 Laboratory instrument integration and automation

The LIS should support integration with laboratory instruments and automated analyzers to enable seamless exchange of test orders and results. At a minimum, the LIS should:

1. Interface with automated laboratory instruments using standard communication protocols.
2. Transmit test orders from the LIS to connected laboratory instruments.
3. Receive test results directly from laboratory instruments without manual re-entry.
4. Associate instrument- generated results with the correct specimen, test order, and patient record.
5. Capture instrument identifiers, test run identifiers, and quality control indicators.

2.3.5 Commodity management

LIS should conform to the standards of the current version of ISO 15189: Clause 4.6 and 5.0 sub clause 5.3.2.4 and ISO 17025: Each test performed in a laboratory requires several different commodities. More complex tests often require more commodities, including equipment. Laboratories manage hundreds or thousands of individual commodities, depending on the number and complexity of the laboratory services provided. Commodity management is a crucial and complex process within the laboratory. The LIS should communicate with existing commodity management systems and may have an integrated commodity management function.

The commodity management information that should be accessible by the LIS includes:

1. Expiry dates for culture media, reagents, stains, and other materials required for laboratory analytical testing activities
2. Monitor stock levels and flag predetermined minimum levels

2.3.6 Reporting

Laboratory reports include summarized information about individual laboratory tests and corresponding results. The LIS should generate predefined and user-defined reports, including:

2.3.6.1 General Laboratory Reports

The LIS should:

1. Generate reports based on the tests carried out by the laboratories and the subsequent results.
2. Generate reports for laboratory management, including process and output reports.
3. Generated reports should include the number of laboratory tests run per day and the number of positive tests for each test carried out.

2.3.6.2 Statistical Analysis

This is the collection, examination, summation, manipulation, and interpretation of quantitative data to discover its underlying causes, patterns, relationships, and trends. Within the laboratory, statistics are used to monitor and verify method performance, and interpret the results of clinical laboratory tests

The LIS should calculate:

1. Sensitivity of a test
2. Clinical specificity of a test
3. Predictive values of a test

2.3.6.3 Disease Surveillance

This is an epidemiological practice by which disease spread is monitored to establish patterns of progression. The main role of disease surveillance is to predict, observe, and minimize the harm caused by outbreak, epidemic, and pandemic situations, as well as increase knowledge about which factors contribute to such circumstances

The Technical Guidelines for Disease Surveillance and Response in Kenya require laboratories to report on diseases of public health priority as defined in the IDSR framework, including:

1. Brucellosis
2. Influenza
3. Schistosomiasis
4. Shigella dysenteriae type 1
5. Tuberculosis (MDR-TB and XDR-TB)
6. Typhoid Fever

2.3.7 Quality management

Quality management incorporates oversight of activities and tasks to maintain operational excellence. Quality management includes creating and implementing quality planning and assurance, and quality control and quality improvement. The LIS and laboratories should support quality management activities through the following functionality:

2.3.7.1 Proficiency Testing

This refers to determining a laboratory's calibration/testing performance, usually by using interlaboratory comparisons. The LIS shall capture and chart the performance of the laboratory in all the undertaken proficiency tests

2.3.7.2 Audits

An audit is an essential part of the quality assurance program of a laboratory and is a means of assessing whether one is achieving set guidelines. The LIS should support the recording of results from assessments by external authorized organizations on their level of conformity to the testing guidelines.

2.3.7.3 Laboratory Licensing

The LIS should support scheduling of inspections and re-inspections and exchange of data with systems that track LIS proficiencies and deficiencies and certification for technologists and the laboratory. The LIS may keep track of the re-inspection dates and license expiry to issue alerts when the processes are due.

2.3.8 Information security

The LIS should support the following functionality:

1. Log all login attempts
2. Provide timestamps for all transactions
3. Support data encryption at rest and in transit

2.3.9 Exchange of electronic data

The LIS should:

1. Be able to consume and output FHIR formatted tests and results.
2. Integrate with the MoH electronic registries.

2.4 Pharmacy Information Systems

Pharmacy Information Systems (PIS) are facility-level information systems, usually computer-assisted, designed to store, manipulate, and retrieve information for planning, organizing, directing, and controlling administrative activities associated with the provision and utilization of pharmacy services.

PIS collects valuable information that helps track patient medication profiles and monitor patients' responses to treatment, ultimately determining medicine effectiveness. They also aid in reducing medication errors through clinical decision support functions that include detection of adverse drug reactions (ADRs) and prescription errors. The functional requirements include:

2.4.1 Prescription Management

1. Capture prescription information in a structured format and receive selected clinical and diagnosis information
2. Facilitate prescription processing including generic alternatives, approved formulary, change or cancellation, medication information, and a register of controlled medicines among others
3. Uniquely identify prescriptions and patients
4. Capture additional patient information including medication records
5. Allow search of patient's medication records, based on government-issued identification number, name, telephone number, unique pharmacy number
6. Capture medication counseling notes
7. Allow for reporting and access to reported ADRs stored on EHRs/EMRs or on the PIS
8. Provide an audit trail of all electronically transmitted prescriptions, indicating all actions and persons who have acted on the prescription

2.4.2 Clinical Decision Support

The PIS should:

i. Issue age-specific warnings for pediatric and geriatric patients
ii. Issue alerts for dose adjustment needed with respect to patient weight
iii. Alert PIS users about:
    - Potential adverse drug reactions and allergies
    - Possible undesirable or unsafe situations, including potentially inappropriate dose or route of administration of a medicine
    - Patients who have missed medicine refills
    - Key warnings
    - Auxiliary labels
iv. Facilitate maintenance of business rules, clinical policies, and guidelines

2.4.3 Inventory Management

The system should:

1. Track product batch numbers, manufacture, and expiry dates
2. Track product movement between the pharmacy, other service delivery points, the pharmacy store, and suppliers
3. Accept, modify and display products' and suppliers' information
4. Capture the cost of the products supplied
5. Manage budgetary allocations, e.g., drawing rights
6. Facilitate quarantine of poor-quality products
7. Provide standard inventory management functions:
    a. Stock taking
    b. Stock receipts
    c. Stock issues (FEFO/FIFO)
    d. Stock ordering
    e. Stock adjustment and redistribution
    f. Losses and disposal
    g. Consumption/usage tracking
    h. Expiry alerts

8. Facilitate definition of maximum and minimum stock and reorder levels, and reorder quantities

2.4.4 Accounting

The PIS should:

1. Access information on products with waivers and exemptions
2. Track the value of products issued to patients by the pharmacy
3. Facilitate the printing of receipts and invoices for medication dispensed to the patients
4. Process and track insurance claims and payments
5. Purchases management
6. Sales management
7. Cash book and Ledger manager
8. General accounting and financial analysis

2.4.5 Report Generation

The PIS shall facilitate generation of the following standard reports:

1. Stock-related reports
    a. Stock / inventory report - shows a list of available products in stock, expired and short expiry items and items out of stock
    b. Consumption reports - by type and department, i.e., in/outpatient
    c. Stock status report - based on quantities in stock, set maximum and minimum stock level parameters and average consumption/usage, e.g., items over- or under-stocked
    d. Re-order report
    e. Order report
    f. Issues reports
    g. Receipts report
    h. Stock movement reports - including slow- and fast-moving products
    i. Stock valuation
    j. Stock variance
2. User Audit trail
3. Prescription volume reports - show the number of prescriptions made within specific time intervals, the number of items issued per prescription and the total number of items dispensed in all the prescriptions
4. Accounting reports - show revenue, costs, and margins over a period of time
5. Patient medicine review - shows listing of previous and current medication for individual patients, progress and outcomes
6. Poor-quality products reporting
7. Adverse drug reaction reporting
8. Medication errors reporting

The PIS shall facilitate generation of the following customized reports:

i. National and pharmacy-related indicators
ii. Program-based reports such as patients by regimen
iii. Patient statistics - show aggregate patient data, e.g., numbers of patients seen at the pharmacy

2.4.6 Medical Therapy Management

The PIS should allow.

i. Identification of patients eligible for MTM
ii. Workflow management and scheduling
iii. Access to medical and lab records
iv. Generation of a Personal Medicines Record
v. Medication Action Planning
vi. Referral
vii. Documentation and follow up

2.4.7 Information security

The PIS system should support the following functionality

1. Log all login attempts
2. Provide timestamps for all transactions
3. Support data encryption at rest and in transit

2.4.8 Exchange of electronic data

The PIS systems should:

1. Be able to consume and output FHIR formatted tests and results.
2. Integrate with the MoH electronic registries.

2.5 Logistics Management Information System (LMIS) Functionality

A Logistics Management Information System (LMIS) is an IT system that plays a leading role in enabling commodity visibility and operational management of a wide-area supply chain operations. An LMIS bridges the health and supply chain operations by enabling re-supply workflows for clinical locations and the vertical programs targeting families of commodities, as well as interfacing with supplier's IT systems to ensure the re-supply process is fulfilled as needed. LMIS tools may have additional capabilities that enhance these resupply workflows and/or add to the maturity of the wider supply chain operations.

2.5.1 Forecasting & Supply Planning

The LMIS should support the national MoH in:

1. Forecasts: Analyze historical data to forecast future demand.
2. Supply Plans: Managing the flow of HPTs through the supply chain, ensuring alignment between demand and supply.

2.5.2 Supplier & Contract Management

The LMIS should support the regional warehouse in:

1. Sourcing: Finding, selecting, and acquiring HPTs from external suppliers or vendors to meet MoH needs

2. Tender Management: Soliciting, evaluating, and awarding contracts or purchase orders for products, services
3. Supplier Information Management: Maintain supplier information and contracts, performance, and compliance

2.5.3 Procurement Management

The LMIS should support the regional warehouse with:

Purchase Orders: Raise document for specific products, services, or materials to be purchased and the terms and conditions of the transaction

2.5.4 Order Management

The LMIS should support the national MoH, regional warehouse, county/sub-county, health facility and community in:

1. Requisition Orders: Initial step in the procurement process, initiating the acquisition of necessary resources to procure products
2. Transfer/Distribution Orders (national MoH, regional warehouse, county/sub-county): Raise document to facilitate the movement of products or materials from one location to another within an organization

2.5.5 Warehouse Management

The LMIS should support:

1. Inbound Orders (national MoH, regional warehouse, county/sub-county): Requests for products from external suppliers or vendors
2. Inventory Management (national MoH, regional warehouse, county/sub-county, health facility and community): Stock Receipts, Stock Issues, Transfers & Adjustments, Stock taking, inventory audit trail
3. Storage Locations (regional warehouse): Manage storage locations for visibility of inventory for pick and pack
4. Shipments (regional warehouse, county/sub-county): Schedule shipments and track delivery progress.
5. Receipts (community): Recording of products received
6. Stock Issues (facility and community): Recording of products issued

2.5.6 Transport Management

The LMIS should support:

1. Delivery Routes (regional warehouse, health facility): Route planning and optimization
2. Proof of Delivery (regional warehouse, health facility): Documented evidence that a shipment or delivery has been successfully received by the intended recipient

2.5.7 Master Data Management

The LMIS should support national MoH and regional warehouse with:

1. Product Master: Comprehensive central repository or database that stores detailed information about the products

2. Facility Master: Comprehensive repository of information about physical facilities
3. Supplier Master: Centralized repository of information about the suppliers or vendors

2.5.8 Track and Trace

The LMIS should support national MoH and regional warehouse with:

1. Verification: Confirmation of the authenticity, integrity, and accuracy of product data as it moves through the supply chain
2. Traceability: Ability to track and trace the movement of products throughout the supply chain, from their point of origin to their final destination
3. Recalls: Ability to remove or collect products from the supply chain due to safety concerns, defects, or regulatory violations
4. Support recall execution workflows, including notifications, tracking of affected stock, and confirmation of recall completion.

2.5.9 Analytics and Reporting

The ability to track key performance indicators, produce standard reports and allow for custom report development and analytics on the data. These requirements would apply to all resource settings. All threshold KPI's should be configurable by the administrator of the system. This includes:

1. Product Quality Adherence
2. Stocked According to Plan (SATP)
3. Inventory Turns
4. Total Supply Chain Cost as % of Distributed Product Value
5. LMIS Order Reporting Rate
6. Closed vial wastage
7. Functional status of cold chain equipment
8. Temperature alarm rates

2.5.9.1 Basic Reports

1. Transactional reports (order, invoice, pick list, packing list, shipment notification, shipment confirmation, proof of delivery, returns with reason code, stock adjustments on physical counts)
2. Inventory reports: product quantity per location (absolute quantity, months, or weeks of stock), product aging (by expiry), closed vial wastage rate, open vial wastagerate4, low stock alert
3. CCE reports: volumetric capacity available (per unit, per location), temperature excursion rates and durations, CCE need attention, CCE non-functional, average CCE downtime, CCE service schedule, service due, service pending, technician responsible, service outcome
4. SMS/email/direct messaging and dashboard notifications for all exceptions and escalation logic for aging exceptions
5. Sorted and filtered lists of facilities, commodities, inventory cards, and transactions for all products, requisitions, shipment notifications and confirmations, and proofs of delivery
6. Forecast reports for time periods & levels: forecasted requirements, constrained requirements (see forecasting & supply planning), future stock positions
7. Data quality, including on-time reporting, and completeness of data (e.g., sites reporting for the period
8. Installed CCE capacity analysis: total available capacity availability and gaps against current and future capacity needs, based on inputted assumptions including supply intervals, vaccine presentations, population growth

2.5.9.2 Performance Reports

1. Full Stock Availability, all tiers
2. Stocked According to Plan, all tiers
3. Stock-out Duration, all tiers
4. On-Time, In Full delivery (OTIF), all tiers
5. Forecasted Demand Ratio (forecast accuracy)
6. Closed Vial Wastage, all tiers
7. Temperature Alarm Rate and (where possible) Average Duration, all units
8. Functional Status and (where possible) Average Downtime of Cold Chain Equipment
9. Coverage Supply Ratio (coverage reported vs. items utilized)

2.5.9.3 Operational Reports

1. System downtime
2. System usage (by user, by team / facility / other)
3. System backup status (success/failure, size, time taken)
4. System utilization (CPU, memory, disk, network).
5. System scheduled jobs status (success/failure, schedule, time taken)
6. Master data accuracy per Product, Supplier, Facility
7. System failures and warnings

2.5.9.4 Custom Reports

1. System allows for a system administrator or power user to customize basic reports to meet their specific needs. In addition, describe the system's capability to integrate with advanced analytics tools such as Business intelligence tools for custom reports and analytics
2. System can produce a report that shows the Inventory disposition of a product based on Funding Source of the original procurement

2.5.10 Information security

The LMIS should support the following functionality:

1. Log all login attempts
2. Provide timestamps for all transactions
3. Support data encryption at rest and in transit

2.5.11 Exchange of electronic data

The LMIS should:

1. Be able to consume and output FHIR formatted tests and results.
2. Integrate with the MoH electronic registries.
3. The LMIS should support integration with automated cold chain monitoring devices

HEALTH INFORMATION EXCHANGE STANDARDS AND GUIDELINES

1.0 Introduction

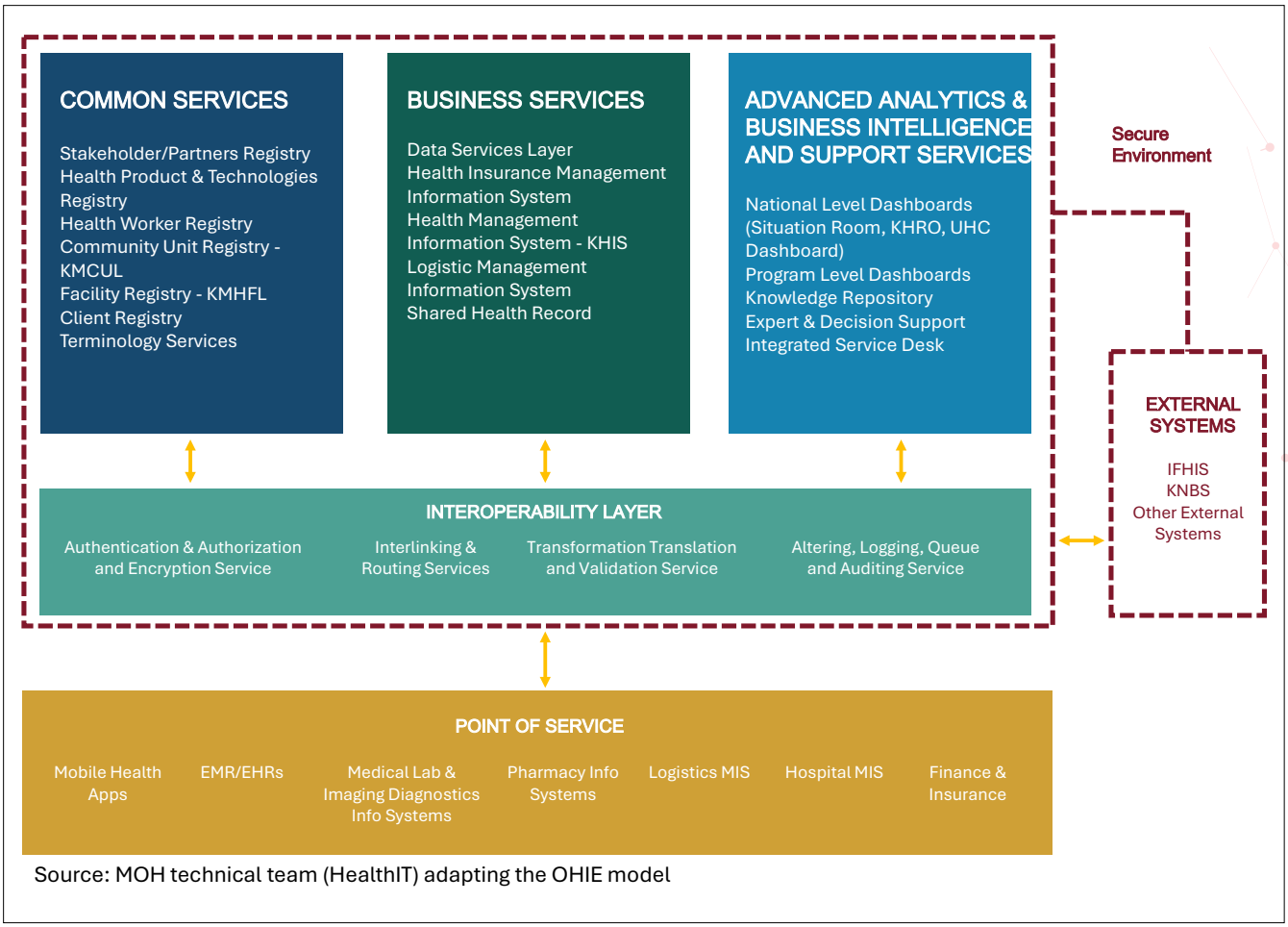
The Ministry of Health developed the Kenya Health Policy (2014–2030), in line with the Government of Kenya's aspiration to improve access to and equity of quality essential health care services and to ensure that the health sector plays its role in the realization of Vision 2030 and attainment of the Sustainable Development Goals (SDGs). Strengthening the health information ecosystem in Kenya has been brought to the fore by the Ministry of Health by optimizing availability and use of information for decisionmaking in the health sector through the implementation of targeted health information systems.

A fundamental concern in health management is the integration of health information across distributed, heterogeneous, and disparate information systems to address the challenge of parallel HIS, some of which do not adhere to the requisite HIS standards. Kenya Health Enterprise Architecture (KHEA) is at the center of facilitating
health information interchange among digital health systems in the health sector.

This document sets out the overarching guidelines for Integration and Interoperability as guided by the Interoperability architecture in the Kenya Health Information Systems Interoperability Framework (2020).

The term "interoperability" describes the ability of two or more information systems or components to exchange information based on standards, and to use the information that is exchanged. Interoperability enables different HIS to work together in and across organizational boundaries to advance the health status of individuals and communities and the effective delivery of healthcare to them (Healthcare Information and Management Systems Society [HIMSS], 2013).

The Kenya Health Interoperability architecture defines a conceptual model that promotes interoperability by design and is anchored in the Open Health Information Exchange (OHIE) framework. This means that for Kenya health systems to be interoperable, they should be designed in accordance with the proposed model and with certain interoperability and reusability requirements in mind.



Source: MOH technical team (HealthIT) adapting the OHIE model

Figure 1 - Kenya Health Interoperability architecture conceptual model

The Kenya Health Information Exchange (HIE) enables the secure electronic sharing of health-related information among different health information systems. The goal of HIE is to facilitate access to and retrieval of clinical data to provide safer, more timely, efficient, effective, and equitable patient-centered care. HIE systems typically involve secure methods for transmitting and storing health information, ensuring patient privacy and data security are maintained. These systems play a crucial role in improving care coordination, reducing medical errors, and enhancing public health reporting.

2.0 Kenya Health Interoperability Architecture Components

The Kenya Health Interoperability architecture describes the interoperability layer along with the adaptation of the Fast Health Interoperability Resource (FHIR) for the Kenyan context. It further highlights the basic HIS components within common services, business processes and Advanced Analytics that will facilitate interoperability between disparate HIS systems.

The Ministry of Health (MoH) Kenya, Health Systems Interoperability Services consists of the following components:

1. Interoperability Layer
2. Kenya Client Registry
3. Kenya National Health Terminology Service
4. Kenya Health Worker Registry
5. Kenya Health Facility Registry
6. Kenya Community Health Unit Registry
7. National Shared Health Record
8. Kenya Health Products and Technologies Registry/Product catalogue

2.1 Interoperability Layer

An Interoperability Layer provides a single point of entry into a HIE, which allows requests to be logged and routed or multicast to the systems that make up the HIE infrastructure[2]. The system should:

1. Provide a central point of access for the services of the HIE. For example, this interface will provide access to the CR, PR, FR and SHR. This central point of access simplifies security management and provides a single-entry point into the HIE.
2. Provide routing functions that allow messages to be routed to the correct service provider systems within the HIE.
3. Provide a central logging mechanism for the messages sent through the exchange. This function should log copies of the messages that travel through the interoperability layer for audit and reporting purposes.
4. Support transformation of messages that travel from the interoperability layer to service provider systems and vice versa if the service provider is not able to communicate in the required format, i.e., provides implementation specific adapters to transform messages from the interoperability layer's internal form to a form that the service provider expects (e.g. SHR, CR, PR).
5. Allow for the routing of messages to the appropriate architecture component or external Point-of-Service system.
6. Performs orchestration tasks for complex transactions to take the burden off client systems. This orchestration may contact multiple service providers within the Health Information Exchange (HIE) on a client's behalf and compile an appropriate response to return it to the client.
7. Support the ability to be extended by allowing additional mediation functions to be added or removed as they are needed.
8. Manage the security of the HIE through authentication (identity verification), authorization (permission to interact with specified HIE components) and encryption and decryption of messages.
9. Capture monitoring statistics, such as transaction loads and performance metrics, and provide a view of these for monitoring the flow of messages through the HIE.

[2] https://wiki.ohie.org/display/CP Interoperability+Layer+Use+Cases+and+Requirements

2.1.1 Fast Healthcare Interoperability Resources (FHIR) Profiles

FHIR (Fast Healthcare Interoperability Resources) is an HL7 standard that defines how healthcare information can be exchanged between different computer systems regardless of how it is stored in those systems. It allows healthcare information, including clinical and administrative data, to be available securely to those who have a need to access it, and to those who have the right to do so for the benefit of a patient receiving care. The standards development organization HL7 (Health Level Seven) uses a collaborative approach to develop and upgrade FHIR.

2.1.1.1 Adaptation of FHIR profiles for Kenya context

The FHIR specification provides a standardized framework consisting of base resources, frameworks, and APIs utilized across various healthcare contexts. Despite its universality, there exists considerable variability between jurisdictions and within the healthcare ecosystem concerning practices, requirements, regulations, education, and feasible actions. FHIR serves as a platform specification, establishing a common foundation upon which diverse healthcare solutions can be developed. However, due to the differing needs of each context, FHIR often necessitates further adaptation. These adaptations involve specifying how FHIR elements and features are tailored to suit specific use cases and environments, ensuring seamless integration and optimal functionality.

The adaptation requirements call for systems to observe:

2.1.1.1.1 Resource Element Utilization Rules

1. Specify which elements of FHIR resources are utilized or excluded based on local requirements.
2. Define rules for adding additional elements to the base specification as needed.

2.1.1.1.2 API Feature Usage Rules

1. Determine which features of the FHIR API are utilized and how they are implemented.
2. Define rules for customizing API functionalities to meet specific requirements.

2.1.1.1.3 Terminology Rules

1. Establish guidelines for the use of terminologies within FHIR resource elements.
2. Define mappings between local terminologies and standard terminologies used in FHIR.

2.1.1.1.4 Context-Specific Adaptations

1. Describe how FHIR resources and APIs are adapted to align with local regulations, practices, and workflows.
2. Specify any modifications or extensions needed to integrate FHIR with existing systems or standards.

2.1.1.1.5 Data Exchange Patterns

1. Define standardized data exchange patterns to ensure interoperability between different healthcare systems.
2. Specify protocols and formats for exchanging FHIR resources securely and efficiently.

2.1.1.1.6 User Interface Requirements

1. Define requirements for user interfaces that interact with FHIR-based systems.
2. Ensure usability and accessibility of interfaces for healthcare professionals and patients.

2.1.1.1.7 Security and Privacy Requirements

1. Specify security measures to protect patient data exchanged using FHIR.
2. Ensure compliance with regulatory requirements and industry standards for data privacy and security.

2.1.1.1.8 Interoperability Standards Compliance

1. Ensure compliance with interoperability standards and profiles defined by regulatory bodies or industry organizations.
2. Facilitate seamless integration with other healthcare IT systems and interoperability networks.

2.2 Client Registry

The Client Registry (CR) is an electronic database that holds the demographic information on clients who receive healthcare services and that aims to accurately match and link records by uniquely identifying individuals. The CR is meant to facilitate the exchange of patient/client information between disparate systems on the Kenya Digital Health Superhighway.

The Client Registry should:

1. Create a unique master record for each patient record in the CR. This unique master record ID can be returned to the source systems if required and depending on the use case.
2. Accept queries for different types of searches using multiple combinations of patient attributes-fuzzy and exact)
3. Allow for deduplication-this happens as part of the registration process.
4. Be able to verify that any national ID binds to valid demographic and biometric data from the IPRS system.
5. Support generation of custom reports e.g. Trend analysis, duplicated reports

2.3 National Health Terminology Services

A Terminology Service serves as a central authority to uniquely identify the clinical activities that occur within the care delivery process by maintaining a terminology set mapped to international standards such as ICD10, LOINC, SNOMED, and others.

The terminology service provides a centralized source for the health information exchange standards and definitions, including terminologies, ontologies, dictionaries, code systems, and value sets. Other HIE components can use these standards and definitions to normalize clinical data and achieve consistent aggregation and reporting. By using Terminology Services, it actualizes semantic interoperability. Semantic interoperability enables accurate, consistent reporting and aggregation of clinical data. It also enables accurate exchange of information among members of the provider community, including labs, clinics, pharmacies, hospitals and imaging centers, which leads to improved patient care decisions.

Terminology Services also support other architecture components such as the Health Facility Registry and Shared Health Record.

The terminology service should:

1. Support import and export of local (e.g., local lab codes) and standard code systems (e.g., LOINC).
2. Support versioning of code systems and value sets - storing and making multiple versions of a code system available via terminology services.
3. Allow import and export of value set definitions and expansions. The import format may vary from a text file containing a list of codes to an FHIR Value Set resource in XML or JSON format.
4. Allow for the import and export of relationships between codes (i.e., concept maps). The import format may vary from a text file containing source and target codes to an FHIR Concept Map resource in XML or JSON format.
5. Expose services that allow for the retrieval and validation of a code, and additional information about the code such as definition and status, from a particular code system (and code system version if provided).
6. Expose services that utilize concept maps to retrieve a target code given a source code within the concept map.

2.4 Health Worker Registry

The Health Worker Registry serves as the central authority for maintaining the unique identities of health workers within the country based on agreed-upon standards.

The Health Worker Registry is a database containing a minimum dataset of details of all health workers working in both the public and private sectors. With multiple and disparate sources of data on health workers, it is a complex task to pull together and maintain a master and canonical list of all health workers in a country. The health worker registry seeks to reduce the complexity of this task by:

Pulling the minimum dataset of health workforce information from the various source data systems.
Merging the source data systems into an authoritative registry of health workers according to a data governance policy.
Allowing queries of health worker information by client systems.

The health worker registry should:

1. Support the ability to query source data systems for updates to health worker data.
2. Support the ability to retain received updates from source data systems.
3. Support the ability to respond to queries on health worker data stored.
4. Be able to send updates to upstream data repositories (such as an Interlinked Registry).
5. Support the ability to maintain old versions of health worker data when it has been updated.
6. Support the collection of data for the following minimum dataset:
7. Have flexible standards-based APIs, based on CSD or mCSD.

2.5 The Kenya Master Health Facility Registry

The Kenya Master Health Facility Registry (KMHFR) is a web-based system which is used to manage health facilities and community health units' data. The role of the Kenya Master Facility Registry is to ensure that all facilities providing services to the citizens are registered in the system and identified by a unique code, and all Community Health Units are identified with a unique code within their link health facility. The Health Facility Registry acts as the central authority to collect, store, and distribute an up to date and standardized set of facility and Community Health Unit data.

The Kenya Master Health Facility Registry should:

1. Support the ability to create, define, and evolve the attributes & associated data dictionary for a registry.
2. Support the ability to create, define, and maintain multi-organizational hierarchies of facilities and related geo-objects.
3. Support the collection of data for minimum facility attributes dataset.
4. The system should support the collection of data for minimum Community attributes dataset.
5. Support the ability to search for facilities/CHUs by attribute.
6. Support facility data curation to manage status changes (closures, openings, service changes/upgrading/downgrading).
7. Support Community health Unit data curation to manage status changes (closures, openings, service changes/functional/Semi functional).
8. Generate standard and customizable reports.
9. Be able to Archive closed health facilities/CHUs.
10. Generate Dashboard and Visualization of Facility and CHUs statistical reports.
11. Enhance standalone modules -Mortuaries, stand-alone labs, pharmacy…etc.
12. Be configurable to allow for the addition of future service needs.
13. Support the ability to visualize the facility/CHU on a map.
14. Allow public access to data relevant to the public (e.g., services provided by a facility).
15. Support the ability to create, define, and maintain multi-organizational hierarchies of facilities/CHUs and related geo-objects (GIS module).

2.6 Shared Health Record

The Shared Health Record (SHR) facilitates the sharing of clinical information between health information systems to enable better patient care, thus improving health outcomes. The Shared Health Record is a means of allowing different services to share health data

stored in a centralized data repository. It contains a subset of normalized data for a patient from various systems such as an electronic medical record or the Laboratory Information Management System. This record is queried and updated between the institutions and systems authorized to do so. The following are the functional requirements:

The shared health record should:

1. Store patient level clinical data that forms a patient's electronic health record.
    a. Store unstructured clinical data such as PDFs and narrative text.
    b. Store structured clinical data such as an encounter with several discrete observations, compatible with a standard exchange format.
    c. Relate clinical information to other clinical information, e.g. annotating/describing a document with discrete observations.
2. Expose services that can receive and save patient clinical data in unstructured form, both text and binary (PDF/image), annotated with sufficient metadata to identify patient/provider.
3. Expose services that can receive and save patient clinical data in a structured form such as CDA documents or FHIR resources.
4. Expose services that can receive and save patient clinical data in a form that contains both structured and unstructured elements.
5. Exposes services that respond to queries for a patient's EHR
    a. Return a specific known document or a list of documents for a patient (as it was submitted).
    b. Return a list of discrete observations for a patient that satisfies specific query parameters. This data can subsequently be used for trending or providing the previous encounters that a patient has had.
    c. Return a full set of clinical information stored about a patient.
    d. Return patient summary - everything the SHR knows about a patient with links to fetch the individual data items.
6. Maintain the context in which the data was submitted.
7. Keep detailed audit logs of all interactions with clinical data.
    a. Keep audit logs of any clinical and demographic data that is stored or changed. Logging who has accessed/viewed clinical information does NOT need to be stored, this is something that an interoperability layer could log.
    b. Record and version updates; records can never be deleted, only marked as such; any previous update should not rewrite old data; no information should ever be removed from the system.
8. Support the ability to export data for secondary use.
9. Provide interfaces/extension points at various stages of the data lifecycle to allow for semantic validation or simple decision support.
10. Allow for storage and retrieval of basic privacy/policy constraints (access control/restrict part of record and restrict entire record).
11. Be able to store identified and predefined observational data mapped to standard reference terminology.
12. Have a mechanism to resolve conflicts if records are submitted more than once.

2.7 Claims Management System

The Claims Management System stores, categorizes, and facilitates the administration of centralized claims and finance related data for care provision to patients within the HIE. The service receives claims/financial data from Point of Service applications (including financing applications acting as a point of service interface outside of other PoS systems) and curates the management of them.

The Claims Management System should:

- Be able to review and assess medical service claims submitted by healthcare providers to determine the eligibility of benefits for patients.
- Implement a standardized benefit structure that clearly outlines the coverage and reimbursement policies for various medical services.
- Verify the eligibility of patients seeking medical services to ensure they are covered by an insurance plan or meet specific criteria for reimbursement.
- Enable the collection of insurance premiums from covered individuals, ensuring timely and accurate payment processing.

- After claims have been approved, initiate the reimbursement process for medical fees incurred by healthcare providers.
- Support various identification formats (e.g., National IDs, Passports IDs, Fingerprint IDs) to avoid duplication and improve data accuracy.
- Use FHIR standards for e-claims interoperability.
- Implement AI-based fraud detection algorithms.
- Be equipped to support the functionalities required for efficient fund management by the chosen fund manager. It should include features for funds disbursement, financial reporting, budgeting, and performance monitoring to ensure effective utilization of resources and transparent financial operations.

2.8 e-Referral Management

A comprehensive health care system used to manage client health care needs by referring clients from an initiating facility to an organization, service, or community unit that can better provide the level of care needed. Effective referral networks should provide linkages across the different levels of the health system, from the community to the tertiary level. This thereby ensures that clients receive the full spectrum of care provided by the health system, regardless of the level at which they physically access health care.

Kenya's referral services framework provides for movement of four categories of elements:

i. ***Client movement:*** considering the different facilities available where current health needs can be addressed in the most efficient and cost-effective way.
ii. ***Expertise movement:*** specialized service providers come to the client to provide services in many ways such as out-reach, screening in a medical camp, or surgeries in remote areas. The movement of expert professionals is from higher levels to lower levels.
iii. ***Specimen movement:*** Movement of Laboratory specimens to specialized facilities, usually for diagnostic purposes, which avoids the need to move the client in the health services system (refer to National Guidelines for Laboratory Specimen Referral Networks, MoH, 2012).
iv. ***Client parameter movement:*** Movement of individual health Information with defined minimum data elements available for the service Client information can be sent to appropriate levels of the health system for supportive diagnosis or management guidance with the use of information and communication technology (ICT) in the health services.

The e-referral system should:

1. The system should be able to generate Standard referral forms for:
   a. Client movement
   b. Client parameter movement
   c. Expertise movement
   d. Specimen movement
   e. In-transit client monitoring form for emergency referrals
2. The Electronic Referral System should be able detect if the patient has missed their referral by checking if an encounter has been received at the Longitudinal Health Record within the time frame indicated in the referral.

HEALTH SECTOR ICT STANDARDS AND GUIDELINES

1.0 Introduction

Article 43 (1) (a) of the Kenyan constitution guarantees that every citizen has the right— to the highest attainable standard of health, which includes the right to health care services, including reproductive health care. The National Health Policy further identifies specific tenets of health systems focus areas that need to be strengthened to enable response to this constitutional requirement. The National health strategic plan specifies ICT as a catalyst to attaining efficiency in multiple facets of the above areas.

As the Health Sector continues to deepen the devolution of health services, risks of adopting a diversified approach where ICT implementations occur without any reference to a common set of standards and guidelines have emerged. This presented challenges in integration at inter and intra-county and across the two levels of government.

Therefore, as departments responsible for Health between the two levels of Government continue to increasingly embrace ICT in service delivery, it is therefore necessary to strengthen a common approach on ICT implementation based on recognized best practices and standards.

ICT capacity in the Public Health Sector has grown as demonstrated by implementation of various HIS systems such as DHIS, MFL, EMR, eCHIS, iHRIS among other systems. ICT infrastructure has improved through the installation of Local Area Networks, National Fibre Optic Network, Data Centres and Increased cellular network coverage and satellite internet from investments by both public and private sectors. These ICT investments have led to improved service delivery and enhanced information exchange within the health sector.

The challenge that persists in delivering ICT services is ensuring consistency in implementation and harmonization of health sector system requirements. The objective of these ICT standards and guidelines is to ensure consistency in ICT initiatives and management to achieve efficiency thereby improving the delivery of healthcare.

The Ministry of Health will continuously enhance its organizational capacity by adopting modern technologies and skills development. These standards will guide both levels of government to ensure that ICT resources are optimally used to achieve efficiency in healthcare delivery.

The standards promote principles that guide implementation of robust ICT infrastructure, Information systems, support services and operational capacity.

The standards and guidelines derive the authority from:

1. Kenya Communications Act 2009
2. E-Government Strategy - 2004
3. The National ICT Policy - 2019
4. Digital Health Act - 2023
5. Data Protection Act - 2019
6. Computer Misuse and Cyber Crimes Act - 2018
7. Kenya Information and Communication Act - 1998
8. Kenya Health Enterprise Architecture Blueprint 2024 -2030
9. Kenya Digital Health Strategy 2025 -2028

Any other relevant legal provision and Government policies that may come into force after initial implementation of these standards and guidelines.

To provide leading edge, integrated ICT solutions derived from identified strategies based on defined technologies and processes for effective and efficient health care delivery and operating excellence.

To maximize MoH ability to realize its Mission – innovatively, creatively, efficiently, and effectively – and to add value to health care delivery services in order to improve health and well-being of Kenyans.

Specific objectives

1. Support the development, implementation, and maintenance of ICT Systems in MoH;
2. Enhance information security of MoH ICT systems.
3. Promote efficient and effective operations and usage of ICT systems within the MoH;

4. Encourage innovations in technology development, use of technology and general workflows within the MoH;
5. Facilitate the development of ICT skills to support ICT systems in the MoH;
6. Promote efficient communication among the MoH's staff and stakeholders;
7. Promote information sharing, transparency, and accountability within MoH and towards the public and other stakeholders.

The ICT standards shall apply to the MoH at the national and county level and its stakeholders in relation to all MoH ICT related operations. This will also cover private health providers through the various regulatory bodies including The Medical Practitioners and Dentists Board, The Pharmacy and Poisons Board, The Nursing Council, the Kenya Medical Laboratory Technologists and Technicians Board among other health regulatory bodies.

This standard shall be guided by the following key principles:

1. Mainstreaming of ICT in the Ministry
2. Integration of ICT systems
3. Adherence to best practices & policies
4. User, customer, patient satisfaction

The overall responsibility of implementing this standard will lie with the Principal Secretary in collaboration with the ICT Governance Committee which will be responsible for the overall strategic management of ICT resources in the Ministry. The committee will draw representation from heads of departments and the head of ICT being secretary. The committee will be responsible for oversight, enforcement and review of the standards and the initiation of ICT projects.

2.0 The ICT Standards

The last published version of the *health sector ICT standards and guidelines*[3] was published in June-2013. This was a comprehensive document that covered 9 domains to consider in ICT adoption and implementation. The areas include:

1. ICT governance
2. ICT Infrastructure
3. Virtualization, thin client and cloud computing
4. Application and systems software
5. Acceptable use of electronic communication
6. IT Security
7. Data back-up and recovery
8. Human resource development
9. Monitoring and evaluation

Subsequently, the Ministry of Information Communication and Digital Economy (MICDE), under the government enterprise architecture (GEA) framework and through ICTA established ICT standards to be applied across all levels of government (ministries, counties, and agencies). This work has identified 12 standards in 6 domains that must be considered. The third edition of the ICT standards was approved in May 2023 and became effective in July 2023. These are valid for 3 years. The defined standard and guidelines domains are:

1. Infrastructure
2. Systems and Application
3. IT Security
4. Electronic Records Management
5. ICT Governance
6. ICT Human Capacity

Following the recent call by MoH to review the existing ICT standards and guidelines, it was evident that MICDE through ICTA has conducted substantial work in developing ICT standards. In addition, the call emphasized the need to identify and adapt what presently exists in defining the revision process. Therefore, the working group focusing on these standards did a comparison between the earlier document developed by MoH and what has been done by ICTA.

Most of the domains that were covered in the health sector ICT standards and guidelines, have been covered under different domains of the ICT standards developed by ICTA. A key component that has not been addressed is the ewaste disposal. This document has adopted practices as guided by the National Environmental Management Authority (NEMA).

The table below summarizes the 6 domains and 12 standards with links to the respective documents for reference.

[3] https://drive.google.com/file/d/1wagGSrccRTOdfUW7np3K0GdUgdCsFpO/view?usp=sharing

S/No	Thematic Area	Standards	Brief Description	Live Link
1	Infrastructure	ICTA.2.1.003:2023 Network Standard	Provides compliant requirements for design, installations, and management of all categories of IT Networks to be deployed in government	https://cms.icta.go.ke/sites/default/files/2023-07/ICT%20Networks%20Standard%202023.pdf
		ICTA.2.2.002:2023 Data Center Standard	Provides compliant requirements for design, installations, and management of government data centers	https://cms.icta.go.ke/sites/default/files/2023-07/Data%20Center%20Standard-Third%20Edition%202023.pdf
		ICTA- 8.003:2023 Cloud Computing Standard	Provides compliant requirements for design, installations, and management of cloud computing infrastructures for government	https://cms.icta.go.ke/sites/default/files/2023-07/Cloud%20Standard%202023.pdf
		ICTA-2.3.002: 2023 End-User Equipment Standard	Provides the minimum specifications for all computing devices being deployed in government	https://cms.icta.go.ke/sites/default/files/2023-07/End-User%20Computing%20Devices%20Standard%202023.pdf
		ICTA. 2.002: 2021: Fibre Optic-Backbone, Metro and Last Mile Infrastructure Standard	This standard sets out minimum requirements for the planning, design, deployment, operation, maintenance, and management of back-bone, metro, and last mile fibre optic cable.	https://cms.icta.go.ke/sites/default/files/2022-08/Fiber%20Standard.pdf
2	Systems & Applications	ICTA.6.003:2023 Systems & Applications Standard	Provides compliant requirements for design, installations and management of all government Software and applications Systems.	https://cms.icta.go.ke/sites/default/files/2023-07/Systems%20%26%20Applications%20Standard-2023.pdf
		ICTA-4.1.003:2023 Electronic Records Management System Standard	Provides compliant requirements for management of government electronic records data	https://cms.icta.go.ke/sites/default/files/2023-07/ERM%20Systems%20Standard%202023.pdf

3	IT Security	ICTA-3.003:2023 Information Security Standard	Provides compliant requirements for design, installations, and management of Information Technology Security in government.	Government ICT Standards
4	Electronic Records Management	ICTA.4.2.003:2023 Electronic records Management Standard	Provides compliant requirements for management of government electronic records and data.	https://cms.icta.go.ke/sites/default/files/2023-07/Electronic%20Records%20Management%20Standard%20-2023_0.pdf
		ICTA-4.3.003:2023: Digitization of public Records	This standard shall guide conversion and the migration of public records at National and County governments to support automation of business processes. It focuses on procedures and methodologies for changing records from one format to another and moving from one media to another.	https://cms.icta.go.ke/sites/default/files/2023-07/Digitization%20of%20Public%20Records%20standard%202023.pdf
5	ICT Governance	ICTA.5.003.2023 ICT Governance Standard	Provides compliant requirements for IT Governance in government. This includes compliance requirements for government IT service providers and Professional Staff.	https://cms.icta.go.ke/sites/default/files/2023-07/ICT%20Governance%20Standard%202023.pdf
6	ICT Human Capacity	ICTA.7.003: 2023 ICT Human Capital and Workforce Development Standard	Provides compliant requirements for development of Human Capital capacity for deployment and support for government ICT infrastructure and services.	https://cms.icta.go.ke/sites/default/files/2023-07/ICT_Human_Capital_and_workforce_development_standard-2023.pdf

2.2 Disposal ICT waste

E-waste (ICT waste) is considered hazardous waste as it contains toxic materials or can produce toxic chemicals when treated inappropriately. Utilization of ICT in health generates e-waste as devices get to the end of useful life. Disposal of ICT waste shall therefore be guided by the regulations and guidelines developed by NEMA. All users of ICT resources supporting health should adhere to the guidelines and regulations as provided by NEMA. All ICT waste must be disposed of by accredited e-waste processors. The details of ewaste disposal are explained in the Guidelines for e-Waste Management in Kenya (December 2010) and the Draft Environmental Management and Coordination (e-Waste Management) Regulations 2013. The disposal guidelines shall be updated as and when updated international standards or NEMA standards become available.

SECURITY, PRIVACY AND CONFIDENTIALITY STANDARDS AND GUIDELINES

1.0 Introduction

Confidentiality and data security are critical principles in the health sector, given the sensitivity of personal health information. This principle requires that personal data must be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing against accidental loss, destruction, or damage.

This document outlines the criteria for ensuring the security of sensitive personal data and is informed by several existing laws, policies, strategies and standards, including the Data Protection Act (2019)[4], ODPC Guidance Note of Processing Health Data[5], the Kenya Health Data Governance Framework (2025 -2028), the Kenya Government Systems and Application Standards (2019)[6], Kenya Digital Health Certification Framework (February 2025), and references global security standards including NIST SP 800-53[7]. The aim is to ensure compliance with international and national regulations for securing sensitive personal data and digital health interventions against unauthorized access.

The NIST Framework offers guidance for organizations looking to better manage and reduce their cybersecurity risk. NIST offers a set of processes that can help organizations measure the maturity of their current cybersecurity and risk management systems and identify steps to strengthen them.

Use of the NIST CSF offers helps to:

- Gain a better understanding of current security risks.
- Prioritize the activities that are the most critical.
- Identify mitigation strategies in alignment with a country's data protection law, strategy and guidelines.
- Evaluate potential tools and processes.
- Measure the Return on Investment of cybersecurity investments.

These standards apply to all entities involved in the **collection, storage, processing, transmission, and disposal** of health data within Kenya, including but not limited to **healthcare providers, insurers, technology vendors, and government agencies.**

The document provides the criteria for four aspects, including:

a. Confidentiality
b. Data protection
c. Training and awareness
d. Risk assessment

All digital systems used to support the delivery of health services and functions are required to maintain the confidentiality of personal health information. This includes ensuring that only authorized individuals have access to the information and that the information is not disclosed or shared without the patient's consent except where required under a court order as stipulated in the Data Protection Act, 2019[8].

2.0 Data Security and Privacy Controls

The data security and privacy controls are based on the NIST Framework and Kenya Data Protection Act. Systems should meet the requirements below.

2.1 Access Control

The systems should:

1. Implement role-based access controls (RBAC) to restrict system and data access.
2. Enforce strong authentication mechanisms, such as multi-factor authentication (MFA), for accessing health information systems.
3. Regularly review and update access permissions to align with the principle of least privilege.

[4] https://www.odpc.go.ke/dpa-act/

[5] https://www.odpc.go.ke/download/odpcguidance-note-on-the-processing-of-health-data/

[6] https://cms.icta.go.ke/sites/default/files/2022-02/Systems%20and%20Applications%20Standard.pdf

[7] https://doi.org/10.6028/NIST.SP.800-53r5

[8] Data Protection Act 2019

For more information review Authentication and authorization- NIST 800-53 (Access controls) and Security and Privacy Controls for Information Systems and Organizations (nist.gov)[9]

2.2 Audit and Accountability

The system should:

1. Establish logging and auditing mechanisms to track access, modification, and deletion of health data.
2. Retain audit logs for an appropriate retention period as per regulatory requirements.
3. Regular audits of access logs are conducted to detect and respond to unauthorized activities promptly.

2.3 Identification and Authentication

The system should:

1. Implement unique user identifiers for individuals accessing health data systems.
2. Employ strong password policies, including minimum length, complexity, and periodic password changes.
3. Utilize biometric authentication where feasible
4. for enhanced identity verification.

2.4 Data Protection

The system should:

1. Encrypt health data at rest and in transit using industry-standard encryption algorithms.
2. Implement data loss prevention (DLP) mechanisms to prevent unauthorized data exfiltration.
3. Establish secure mechanisms for data backup, replication, and recovery to ensure data availability and integrity.
4. Keep all software and systems up to date with the latest security patches and updates.
5. Establish a patch management process to regularly identify, prioritize, and apply patches to mitigate known vulnerabilities.
6. Configure systems, networks, and devices securely according to industry best practices and security standards.
7. Disable unnecessary services and ports and apply strong passwords and access controls to prevent unauthorized access.

2.5 Incidence Report

The owner of the system should:

1. Develop and maintain an incident response plan outlining procedures for detecting, reporting, and responding to security incidents.
2. Establish a dedicated incident response team with clearly defined roles and responsibilities.
3. Regular drills and exercises should be conducted to test the effectiveness of the incident response plan and to keep updated reports.
4. Attacks (successful or not) shall be reported to the DHA.

2.6 Data Recovery

The system owner should:

1. Implement a comprehensive backup strategy that includes regular backups of critical data.
2. Ensure backups are stored securely, preferably in an off-site or cloud-based location to prevent loss in case of physical damage to the primary data storage.
3. Determine the frequency of backups based on the criticality of the data and the rate of change.
4. Critical data may require more frequent backups, while less critical data can be backed up less frequently.
5. Develop a comprehensive disaster recovery plan outlining the steps to be taken in the event of data loss or a cybersecurity incident.
6. Test the disaster recovery plan regularly to ensure its effectiveness and identify any areas for improvement.
7. Implement mechanisms to verify the integrity of backup data to ensure it has not been tampered with or corrupted.
8. Use checksums or hash functions to validate data integrity during backup and recovery processes.

[9] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

9. Maintain thorough documentation of data recovery activities, including backup schedules, recovery procedures, and testing results.
10. Generate regular reports on backup and recovery activities for auditing purposes and to demonstrate compliance with regulatory requirements.

2.7 Security Awareness and Training

The system owner shall:

1. Develop training materials and provide comprehensive training programs to educate system end users on cybersecurity best practices and privacy policies.
2. Promote a culture of security awareness through regular communications, newsletters, and training sessions.
3. Ensure that all personnel handling health data receive appropriate training on data protection measures and regulatory requirements.

2.8 Risk Assessment

The system owner should:

1. Conduct regular risk assessments to identify and mitigate cybersecurity threats and vulnerabilities. Best practice is to conduct cybersecurity audits regularly and consistently to ensure effective security measures.
    a. The frequency of these audits can vary based on factors such as regulatory requirements, risk assessments, technology updates, and available resources. Generally, audits should occur on a regular schedule, such as quarterly or bi-annually, with additional audits triggered by significant events like infrastructure changes or compliance mandates.
    b. Budget and resource considerations also play a role, as MoH balances the benefits of more frequent audits against associated costs. Continuous monitoring solutions can complement periodic audits by providing real-time insights into security posture, enhancing overall cybersecurity resilience.
2. Establish a formal authorization process for granting system and data access based on risk assessments. This includes implementing a structured procedure for determining who can access information systems and data, considering the potential risks associated with such access.

2.9 Compliance with Regulations

The system owners should:

- Ensure compliance with the privacy and security regulations stipulated in the Kenyan Constitution, the Data Protection Act 2019 and the Digital Health Act of 2023 through independent assessments and audits.

2.10 Physical & Environmental Security

The system owner shall:

- Put measures to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment[10].

2.11 Cloud Security

The Ministry, Counties, Departments, and private health sector entities shall:

- Ensure on demand availability of computer data storage and computing power system resources without direct active management by the user.

[10] https://cms.icta.go.ke/sites/default/files/2022-06/Information-Security-Standard.pdf

3.0 Compliance and Enforcement

Entities subject to the Security, Privacy, and Confidentiality Standards must demonstrate compliance through regular assessments, audits, and certifications. Non-compliance may result in penalties, fines, or other enforcement actions as prescribed by relevant regulatory authorities.

4.0 Review and Revision

The Security, Privacy, and Confidentiality Standards shall undergo periodic review and revision to accommodate changes in technology, regulations, and emerging cybersecurity threats. Feedback from stakeholders and industry experts shall inform the continuous improvement of this standard.

5.0 Reference Resources

This document was developed with reference to the following documentation.

1. Kenya cyber security strategy 2022[11]
2. Data protection Act 2019[12]
    a. Regulation 2021
    b. Data controllers and processing regulation 2021
    c. Clients handling and enforcement procedure 2021
3. Digital Health Act 2023[13]
4. Kenya Health Data Governance Framework 202314
5. Computer Misuse and Cybercrime Act 2018
6. Computer Misuse and Cybercrime (Critical information infrastructure and cybercrime management) Regulation 2024[15]
7. Kenya Health Sector Data Protection and Privacy Policy 2023 Draft
8. Critical Information Infrastructure Protection gazette notice[16]
9. National Institute of Standard Technology framework (NIST)[17]
10. Digital Health Superhighway - Draft Technical Requirements (of 25/08/2023)
11. Government ICT Standards Information Security Standard (Second Edition 2019)[18]

---

[11] https://ict.go.ke/wpcontent/uploads/2022/10/KENYACYBERSECURITY-STRATEGY-2022.pdf

[12] http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

[13] http://www.kenyalaw.org:8181/exist/rest//db/kenyalex/Kenya/Legislation/English/Acts%20and%20Regulations/D/Digital%20Health%20Act%20-%20No.%2015%20of%202023/docs/DigitalHealthAct15of2023.pdf

[14] https://drive.google.com/file/d/1zy46cLSWbAiK2HZEWyYfUA46rIvOs7v/view?usp=sharing

[15] https://nc4.go.ke/the-computer-misuse-and-cybercrime-critical-information-infrastructure-and-cybercrime-management-regulations-2024/

[16] https://nc4.go.ke/the-kenya-gazette/

[17] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[18] https://cms.icta.go.ke/sites/default/files/2022-06/Information-Security-Standard.pdf

Appendix: Contributors

The coordination and development of this document was a collaborative effort led by the MoH in collaboration with its implementing partners. The key contributors to the document were:

Editing		Design
Dr. Nancy Njeru	George Owiso	Brian Ogutu
Waigumo G. Kiragu	Evans Munene	

Contributors

Ministry of Health

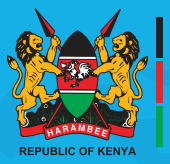
Dr. Bernard Langat	Nancy Amayo
Dr. Ryan Nyotu	Gilbert N. Mboro
Dr. Job Nyangena	Paul Malusi
Dr. Joyce Wamicwe	Waigumo G. Kiragu
Dr. Wesley Ooga	Samuel Kamau
Dr. Martha Muthami	Susan G. Kihiu
Dr. Jeremiah Mumo	Dr. Tracy Njonjo
Diana Kamar	Dr. Jarred Nyakiba
Sophy Karanja	

Council of Governors

Meboh Atieno

Partners

Dr. Jacob Odhiambo	Eric Ejimba
Stephen Wanyee	Lawrence Kimathi
Margaret Ndisha	Dr. Nelly Nyaga
Sam Wambugu	Joseph Warero
Dr. Ramona Koech	Gitahi Ng'ang'a
Joan Ngéthe Cherono	Kirui Lesley Githinji
Samuel Kang'a	Dr. Emma Waiyaiya
Derick Lungáho	Onesmus Kamau
Winfred Nzioka	Charles Brian Bett
Charles Bin Atelu	Danson Koske
Dr. Karimi Muchiri	Patrick Wangai
Dr. Calvine Lwaka	Shalin Moraa



MINISTRY OF HEALTH

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