MINISTRY OF HEALTH

Health Sector Unique Identification Framework

August 2022

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

Table of Contents

List of Figures

List of Tables

DEFINITIONS

Health Facility: The whole or part of a public or private institution, building, or place, whether for profit or not, that is operated or designed to provide inpatient or outpatient treatment, diagnostic or therapeutic interventions, nursing, rehabilitative, palliative, convalescent, preventative, or other health services (Health Act, 2017).

Hospital: A healthcare institution that has organized medical and professional staff, inpatient facilities, and delivers medical, nursing, and other related services 24 hours a day, 7 days a week.

Deterministic Matching: An identity-matching approach based on patient attributes that are known to belong strictly to individual patients or a small, closely related group of patients.

Probabilistic Matching: An identity-matching approach based on patient attributes that are known to belong to many unrelated patients.

Huduma Namba: A unique and permanent personal identification number assigned to every resident of Kenya at birth or upon registration and only expires or is retired upon the death of the individual.

Interoperability: The ability of disparate information systems to exchange and use information in a coordinated manner, within and across regional and national boundaries.

Patient: Any recipient of health care services performed by trained health service providers.

ACRONYMS

API	Application Programming Interface
CCC	Comprehensive Care Center
CDOH	County Directors of Health
CHIS	Community Health Information System
COH	Chief Officer of Health
CECM-Health	County Executive Committee Member for Health
CHMT	County Health Management Team
CR	Client Registry
CSO	Civil Society Organization
DB	Database
DHP	Digital Health Platform
DP	Development Partner
EHR	Electronic Health Record System
EMR	Electronic Medical Record
FBO	Faith Based Organization
FHIR	Fast Healthcare Interoperability Resources
HIE	Health Information Exchange
HI-ICC	Health Information Interagency Coordinating Committee
HIS	Health Information System
HL7	Health Level 7
HMIS	Hospital Management Information System
HSIGCF	Health Sector Intergovernmental Consultative Forum
HTTPS	Hypertext Transfer Protocol (Secure)
ICC	Interagency Coordinating Committee
ICT	Information and Communications Technology
ID	Identifier
KHIS	Kenya Health Information System
KMHCR	Kenya Master Health Client Registry
KMHFL	Kenya Master Health Facility List
KMPR	Kenya Master Patient Registry
KPR	Kenya Patient Registry
LIS	Laboratory Information System
LMIS	Logistics Management Information System
LPR	Local Patient Registry
M&E	Monitoring and Evaluation
MOH	Ministry of Health
MPI	Master Patient Index
NGO	Non-Governmental Organization
NHIF	National Health Insurance Fund
NIIMS	National Integrated Identity Management System
PHR	Personal Health Record

PIS	Pharmacy Information System
PKI	Public Key Infrastructure
REST	Representational State Transfer
RIS	Radiology Information System
SHR	Shared Health Record
SRS	Software Requirements Specification
SSL	Secure Sockets Layer
TB	Terabyte
TLS	Transport Layer Security
TTC	Thematic Technical Committees
TWGs	Technical Working Groups
UHC	Universal Health Coverage
UI	User Interface
UPI	Unique Patient Identification
UUID	Universally Unique ID
VPN	Virtual Private Network

FOREWORD

A critical component in the government's effort to deliver universal health care to the population is its ability to uniquely identify everyone living within the country's borders. Unique identification of patients is a precursor to provision of focused health care and a requirement in providing high quality care. Holistic and historical information about a patient is easy to track especially for longitudinal follow-up of patients as more patients survive for longer periods due to advancement in medical care.

Although there exist various laws and institutions under which citizens' registration and identity data is managed such as the Civil Registration and Vital Statistics and Integrated Population Registration System, there is currently no framework to inform the implementation of unique patient identification.

In keeping with the Kenya Constitution to ensure that every Kenyan has access to high-quality healthcare, along with the aspiration to provide health coverage for all under the Universal Health Coverage agenda, Unique Patient Identification will be the driver of improved medical record-keeping, especially as more facilities adopt digital health records so as to progressively advance the health of Kenyans to the highest standard.

Correctly and unambiguously identifying patients is vital for the delivery of healthcare, administrative processes, information management, follow-up, and preventive care. The Kenya health sector has experienced considerable growth in information systems that support the delivery of health services with major efforts to create a unified health information system as represented in the Kenya Health Enterprise Architecture.

This Unique Patient Identifier (UPI) Implementation Framework is aimed at providing the necessary guidance to inform unique patient identification strategies that will ultimately facilitate higher quality healthcare services for all Kenyans.

Ms. Susan Mochache, CBS
Principal Secretary, Ministry of Health

August, 2022

ACKNOWLEDGMENTS

The Unique Patient Identification Implementation Framework has been developed through a consultative and participatory process that included many partners and stakeholders involved in the implementation of Health Information Systems. The Ministry of Health (MOH) acknowledges the contributions, commitment, and technical support from all stakeholders who participated in the face-to-face meetings and the many virtual meetings that culminated in this final framework document.

Our appreciation goes to the officers in the Ministry of Health Directorate of Health Policy, Research, and Monitoring & Evaluation and the Ministry of Interior and National Government Coordination who steered the review and writing process under the leadership and coordination of Dr. Joseph Sitienei. Our gratitude also goes to national MOH officers from various divisions for their dedication and commitment during the writing process. We appreciate the MOH leadership who provided an enabling environment for the development of this document and to the Council of Governors who through County stakeholders participated in reviewing and validating the framework document.

Finally, we are indebted to the generous financial support from the American people under the United States President's Emergency Plan for AIDS Relief (PEPFAR) through the US Agency for International Development (USAID) Cooperative Agreement No. AID-615-A-12-00001 with Moi Teaching and Referral Hospital as part of the AMPATH Plus project. The Ministry wants to thank the University of Washington's International Training and Education Center for Health (I-TECH Kenya) who provided technical coordination for the development and design of this framework document.

Dr. Patrick Amoth, EBS
Ag. Director General

August, 2022

PART I:
HEALTH SECTOR UNIQUE IDENTIFICATION FRAMEWORK

INTRODUCTION

The Constitution of Kenya (2010) recognizes health as a fundamental human right. Article 43(1a) stipulates that every person has the right to the highest attainable standard of health, which includes the right to healthcare services, reproductive health, and emergency medical treatment. To meet this and other national and international commitments, Kenya is under obligation to craft the necessary laws, policies, and standards to achieve quality, equitable, and affordable healthcare for its citizens. In 2018, Kenya adopted the Big Four Agenda, with Universal Health Coverage (UHC) as one of its pillars. UHC aspires to provide all citizens with accessible, equitable, and affordable health care.

The government has moved to establish a national person identification (ID) process for storing and using identification data which is anchored on the National Integrated Identity Management System (NIIMS). This database will also be utilized as a reference point for national development initiatives, including UHC.

Unique Patient Identification (UPI) is not a new phenomenon in the health sector. As the country moves towards the achievement of UHC, there is a need to ensure that patients can access quality, secure, and affordable care in any health facility across the country. While the government is continuously investing in improving health infrastructure, medical supplies, equipment, digital health technologies, and human capacity, the lack of a supportive framework to facilitate the seamless exchange of patient information to enable quality care, treatment, and referral across the health services and health facilities will hamper the delivery of quality and affordable health care. There are several disparate health information systems currently in use. Coupled with the paper-based systems, patients' data continues to exist in silos of information systems and service providers are not able to use the information to plan for comprehensive patients' treatment and management due to the absence of a coordinated infrastructure to facilitate the sharing of electronic health records (EHRs). Moreover, these scenarios hamper proper and comprehensive health planning as data is fragmented and prone to aggregation errors.

One of the key challenges to consistently and reliably provide high-quality health care is having the ability to uniquely identify patients and their longitudinal medical records. The inability to identify a patient correctly hinders both the tracking and treatment of patients, while at the same time causes disruptions to care, serious medical errors, inefficient use of resources, and lack of accountability. Leveraging the government's initiative for a national person identification (ID) process, UPI will offer the means to identify patients within the healthcare system across the country.

Establishing a UPI system in Kenya will allow the government to:

- Improve quality, safety, and access to care by ensuring that everyone is correctly identified. This will enable healthcare providers to collect and retrieve the necessary information to deliver optimum care at any service delivery point across the country.
- Promote the efficient use of health care resources through better tracking of patients across the continuum of care and across the healthcare system, and by improving scheduling, billing, and insurance benefit claims.
- Maintain a centralized repository of all patients within the Kenya health sector. This will support the correct and unambiguous identification of patients at service delivery points, thereby promoting the quality,

safety, access, and affordability of health care by facilitating data exchange with health, financial, and other sector-specific information systems.

- Maintain a database of accurate statistics devoid of multiple counts for effective and efficient planning.

INTENDED AUDIENCE

This document is intended for health policy makers, technology developers, health service implementers, and health managers. Stakeholders in the health information system (HIS) sector, especially potential users of the Client Registry (CR), are also encouraged to use the document. Technology developers will find valuable information on what the Kenya Patient Registry (KPR) is, what it should do and how it relates to other existing digital interventions in the health sector.

Implementers and HIS stakeholders, on the other hand, will find useful information on how KPR will be deployed and used by different user classes. This knowledge is useful for taking the appropriate steps to prepare for the deployment of the system, including but not limited to updating their own HIS products to incorporate the features required to interface with the CR. On their part, managers will find the information in this document useful for defining the scope of work necessary to actualize the CR, as well as plan and mobilize the resources required for project execution.

CURRENT POLICY ENVIRONMENT

There are numerous policies, guidelines, and standards under which the implementation of UPI has been anchored.

The Kenya National eHealth Policy 2016-2030v recognizes the need for Shared Health Records (SHRs) through the development of a Kenya Master Patient Registry (KMPR) that includes interoperability with Electronic Medical Records (EMR), Personal Health Records (PHR), and Terminology Services (TS). The privacy and confidentiality of the patient identity and health profile will be implemented as per the eHealth policy VI, Health Act, 2017vii, and the Data Protection Act 2019viii.

The Kenya Health Enterprise Architecture ix specifies that the KMPR will include a universal healthcare identifier and provides guidance for uniform patient identification across the information systems that manage patient-level data.

The Data Protection Act (No. 24 of 2019) provides for the collection of personal data by a data controller or a data processor either directly or indirectly. It also recognizes health data as sensitive and gives provisions for its collection, storage, and processing. Under the Act, this data shall only be retained as long as reasonably necessary to satisfy the purpose for which it is processed.

Section 11 of the Health Act, 2017 further provides for confidentiality, stating that "Information concerning a user, including information relating to his or her health status, treatment or stay in a health facility is confidential except where such information is disclosed under a court order or informed consent for health research and policy planning purposes."

Section 103 of the Health Act, 2017 allows for "eHealth to be a recognized mode of health service" making provision for services such as telemedicine and an electronic referral system. In addition, the Act gives provision for the establishment and maintenance of a comprehensive integrated health information system.

The Health Act, 2017 II (10) provides for information dissemination and states that "The national government, county governments and every agency having a role or responsibility within the National Health System, shall ensure that appropriate, adequate, and comprehensive information is disseminated on the health functions for which they are responsible."

The Huduma Namba may also be utilized for the registration and notification of births and deaths occurring within Kenya. The Kenya Health Information Systems Interoperability Framework xi, recommends that the KMPR is the definitive source for a patient's identity, facilitating the unique, accurate, and reliable identification of individual patients.

Similarly, identification of patients in health care has been the subject of standards development by international standards organizations such as the International Organization for Standardization xii, the Integrating the Healthcare Enterprise, UNAIDS guidance for countries adopting national health identifiers xiii, and OpenHIE. This implementation framework refers to these standards regularly, applying them to the Kenyan context and describing UPI implementation in the context of the applicable legislation, policies, and standards.

OBJECTIVES OF UNIQUE PATIENT IDENTIFICATION

The objectives of UPI are as follows:

- To uniquely identify patients for the collection and retrieval of the necessary information to deliver optimum health care (e.g., diagnosis, treatment, blood transfusion, medication)
- To undertake the health administrative functions related to providing health care (e.g., filtering for eligibility for specific services, reimbursement of claims, billing, payment)
- To identify an individual in data exchange transactions between disparate HIS
- To improve the ability to track patient and population health metrics across the health sector to promote the efficient use of resources and improve health outcomes
- To enhance the protection of privacy and confidentiality for all patient information

SECTION 1: DEFINITION, GENERATION, AND MANAGEMENT OF UPI

1.1 Background

UPI refers to the ability to distinguish each individual patient correctly and unambiguously from all other patients in the population for health care purposes and solely for that. It relies on one or more personal attributes by which an individual may be recognized and positively identified within the healthcare system. These attributes include name, gender, date of birth, telephone number, physical address, biometric data, and government or organizationally issued identity numbers. In turn, these attributes are mapped to a single UPI that serves as a static and permanent reference to an individual patient record across the entire health system.

1.2 Rationale

As Kenya marches toward digitizing health data in all facilities to expedite more efficient reporting and meet the aspirations of the Health Act, 2017, this UPI Framework will provide health sector decision makers with important background information on UPI and a road map for the implementation and operationalization of the UPI at various levels of the health system.

Establishing the UPI is a crucial step toward the development of Health Information Exchange (HIE), which will enable data sharing between various systems within the health sector. This framework will help lay the foundation for HIE in Kenya.

1.3 Purpose of Unique Patient Identification

UPI has utility at various levels of health care provision. These include the patient level, service delivery level, and public health level, as described below:

- **Patient Level**: UPI improves patient management and quality of care by enabling the sharing of health records to inform clinical decision making across the continuum of care. This improves safety by reducing the risk of medical errors (e.g., wrong medication or surgical procedures) while strengthening longitudinal care of patients
- **Service Delivery Level**: UPI promotes efficiency in healthcare delivery by speeding up the provision of health services including administrative tasks, supports the referral network through real-time identification of patients in relation to services needed, and optimizes resource utilization (e.g. avoiding unnecessary or repeated procedures)
- **Public Health Level**: UPI facilitates disease surveillance (e.g., during disease outbreaks), promotes data quality by eliminating double counting of cases, and supports research and targeting of interventions and resources

1.4 Characteristics of a UPI

A robust UPI system must be backed by a fit-for-purpose unique identifier that serves as the index for individual patient records. Such a unique identifier should satisfy the following characteristics:

- **Distinctive**: Each identifier must be associated with only one individual patient, i.e., two or more patients should not share the same identifier

- **Non-disclosing**: The identifier itself, on its own, must not contain any personally identifiable information or recognizable patterns that identify the patient outside of the patient identification system (e.g., name, telephone number)
- **Invariable**: Once generated and assigned to a patient, the UPI should not change throughout the life of the person
- **Ubiquitous**: Data belonging to any given patient should be identified using the same unique identifier across the healthcare system
- **Verifiable**: It must be possible to verify that a given UPI is associated with the patient it is claimed to be
- **Canonical**: The identifier should follow a standardized format across the entire health system

1.5 Scope of Unique Patient Identification

The UPI system will identify all persons seeking health care services at all levels of service delivery including public and non-public health facilities. National Identifiers such as National ID, Huduma Numba, passport number, birth certificate number, NEMIS, Alien ID, National Health Insurance Fund (NHIF) ID, National Social Security Fund (NSSF) ID, and birth notification number will be added to the KMPR by recording them as one of many possible personal attributes associated with individual patients in the national registry. For example, a patient may have multiple government issued identification numbers under which they have received health services but would only have a single unique identifier to which the multiple identification numbers are attached. In this way, local identification systems do not need to be discarded, but rather integrated with the UPI system. The unique identifier will be assigned at the earliest possible opportunity to every person seeking healthcare services and will be used in subsequent visits.

1.6 Functional Requirements

1.6.1 UPI Generation

Patients possess a wide range of attributes that identify them. These include names (i.e., first name, second name, surname, and even nicknames); postal and physical addresses; telephone numbers; national identity card numbers (e.g., Huduma Namba); biometrics (e.g., fingerprint and iris scans); and important dates (e.g., date of birth or date of registration). For this reason, the UPI system will accommodate multiple patient attributes. The use of multiple attributes serves to identify the person if one or more attributes are missing or damaged.

However, tracking and storing individual patient records using multiple attributes is both inefficient and unreliable. It would necessitate storing all a patient's attributes every time new information about them is generated (e.g., during a clinical encounter). Because the same information would be repeated across multiple database records, alterations (e.g., a name change due to marriage) would need to be propagated across each system, making the system error-prone and inefficient.

Table 1 - Sample Clinical Encounter Table

Name	ID No	Tel no	Encounter Date	Symptoms
Alice Kenyan	12345678	0700XXXXXX	Jun 1, 2020	Headache, cough
Alice Kenyan	12345678	0700XXXXXX	Jun 15, 2020	Running nose, fever

Table 1 is a sample Clinical Encounter table that shows a contrived clinical encounter where the substantive data (i.e., date and symptoms) is tracked using multiple patient attributes (i.e., name, ID number, and telephone number). Note that besides being repetitive, a simple alteration (e.g., name change) would necessitate the modification of both rows. In the real world, hundreds or even thousands of records could be affected.

The problem is solved by assigning a static UPI that is mapped to a single record listing the other attributes associated with the patient. Any other clinical information in the patient's health record utilizes that unique identifier to reference the patient to which that data belongs. That identifier permanently references the patient within the system forever, regardless of changes to their attributes. The UPI system provides a mechanism for attributing the unique identifier to the associated patient. It also provides the reverse capability, that is, given one or more of the patient's attributes, the system can resolve them to the associated unique identifier, and the patient.

Table 2 - Sample Patient Table

UPI	Name	ID No	Tel No	Encounter Date
123e4567-e89b-12d3-a456-426614174000	Alice Kenyan	12345678	0700XXXXXX	Jun 1, 2020

Table 2 shows a sample patient table that splits the previous clinical encounter table into two, so that common patient attributes are stored in separate patient tables. Within this table, a unique identifier is assigned to the patient. This identifier forms the basis for identifying the individual encounter records associated with the patient.

Table 3 - Improved Encounter Table

UPI	Encounter Date	Symptoms
123e4567-e89b-12d3-a456-426614174000	Jun 1, 2020	Headache, cough
	Jun 15, 2020	Running nose, fever

Table 3 is an improved encounter table that only needs to include the UPI (i.e., 123e4567-e89b-12d3-a456-426614174000). Unlike the previous example encounter table 2, a change in patient attributes is recorded in the index record associated with the patient in the patient table and no longer needs to be propagated across encounters.

There are two possible approaches to generating UPIs:

1. Centralized UPI Generation
2. Distributed UPI Generation

For implementation in Kenya, a distributed UPI generation approach will be used. In this approach, UPIs will be generated at the point of assignment (e.g., health facility), without any reference to a central authority. With this strategy, the main problem to be solved is that identifiers generated independently at multiple service points must not collide (i.e., they cannot result in a circumstance where the same identifier is associated with two or more separate patients).

Universally Unique Identifiers (UUIDs) are the standard way to identify entities in a distributed environment. Also known as Globally Unique Identifiers, UUIDs offer a mechanism for generating virtually, UUIDs without the need for central authority or coordination between the parties generating them.

Different methods of generating UUIDs exist, but they all rely on a random component that greatly minimizes the odds of identifier collisions. While the probability that a UUID will be duplicated is not zero, it is close enough to be statistically unlikely.

This means that regardless of where a UUID is generated, it is, for all practical purposes, guaranteed to be unique across the entire population. The proposed KMPR design proposes to use UUID Version 4 which is designed to minimize the probability of generating a duplicate to as low as one in a billion for every 103 trillion UUIDs generated.

Using a UUID as the unique identifier for patients offers two advantages: the first is that the identifier can be generated in real-time using an electronic system at the service point without reference to a central authority and still be ensured to be unique across the entire healthcare system; and secondly, a UUID-based identifier is effectively random and contains no identifiable information about the entity that it references.

This reduces the problem of de-identifying public health datasets to simply stripping personal attributes and maintaining the unique identifier. This way, while records belonging to one individual can be identified, the individual patient's identity cannot. For the above reasons, a distributed UUID system of identifier generation is the approach being adopted by Kenya in this UPI Framework.

1.6.2 Patient Identification Process

Patient identification is the process of correctly and unambiguously matching a patient to appropriately intended interventions and communicating information about the patient's identity accurately and reliably throughout the continuum of care. A typical use case is when a patient presents at a health facility for clinical care, the care provider may wish to retrieve the patient's data from a local EHR system, or a SHR database hosted remotely. To do so, the care provider will first determine the patient's identity. In other words, the provider will first establish the patient's unique identifier to use to retrieve the patient's record from the database.

The specific identity determination strategy used by the care provider depends on the personal information attribute in the patient's possession. On the other end of the spectrum, the patient may not have any identifying attributes at all (e.g., in the case of an unconscious individual with no identification documents on them).

In between these two extremes, a patient could be in the possession of any number of personal identifying attributes such as names, biometric data, government issued identification documents, date of birth, etc. The specific circumstances dictate the pathway for determining their identity.

In general, two specific strategies of identity determination may be used: deterministic identity resolution and probabilistic identity resolution.

1.6.3 Deterministic Identification Process

Deterministic identity resolution is an identity resolution approach based on patient attributes that are known to belong strictly to individual patients or a small, closely related group of patients. These attributes are not randomly distributed across the population, and each one on its own yields an extremely high degree of certainty when resolving patient identities. Examples of deterministic attributes include government issued identifiers, biometrics, and verified telephone numbers. Because of their high degree of certainty, any deterministic attribute may be relied upon on its own for identification.

Consider, for example, a patient who presents with a government issued identifier such as the National ID or Huduma Namba. A reasonable assumption is that any valid Huduma Namba is associated with one and only one citizen. As a result, to the extent that the national identifier has previously been recorded in the KMPR, resolving a patient's identity using their government issued identifier is straightforward, as a search of the registry would typically yield only one match, or at most a few matches of closely related individuals who can be disambiguated manually, using common personal attributes such as names, sex, and age. The same logic applies to other deterministic attributes such as biometrics and telephone numbers.

1.6.4 Probabilistic Identification Process

Probabilistic identity resolution is an identity resolution approach based on patient attributes that are known to belong to many unrelated patients. These attributes are randomly distributed across the population, and each one yields a low degree of certainty when resolving patient identities. However, a combination of probabilistic attributes can yield an acceptable degree of certainty for identity resolution. Examples of probabilistic attributes include personal names (first, second, last etc.,), sex (male or female), and dates of birth. Because of their low degree of certainty, it is always necessary to use a combination of probabilistic attributes to increase the degree of certainty during identity resolution.

Consider, for example, a patient who presents with no identification documents, and has neither a telephone number nor any biometric data stored in the CR. The process for resolving such a patient's identity is more complex than that of resolving the identity of a patient who presents with a government issued identifier. In this case, the care provider could search for the patient's record in the registry using their first name, say, Alice. But the name Alice is randomly distributed across the population and could yield hundreds of thousands of matches. To get around this problem, the doctor must augment the search with additional information like second name, last name, date of birth, sex, and/or mother's name. As a result, the original large set of patients named Alice shrinks to a much smaller set of patients named Alice Auma Omolo born on 1st January 1980 and whose mother is called Beatrice Nyambura, making identification a lot more straightforward. In practice, probabilistic matching also considers common name misspellings, as well as dates that are off by short duration. This is commonly referred to as fuzzy matching.

1.6.5 Identify Duplicate Patients

As with any software application, a UPI system is bound to have occasional errors during its use. Among the most common is the creation of duplicate patient records in the CR. This occurs when one individual patient in the real world is recorded as two separate patients in the database. Probable causes can range from process violations, technical faults, or even a deliberate falsification of personal information by the patient.

Duplication is a fundamental problem for both patient level and public health data.

At the patient level, duplication can lead clinicians to miss or combine critical data in the patient's health history, which can affect their decision making while providing care. At a public health level, duplication leads to double counting, thereby undermining data quality and the veracity of the resulting decisions and interventions, such as allocating resources or tracking disease outbreaks.

The UPI system, therefore, must account for this reality by providing the necessary means for identifying and correcting duplicates when they occur. This process is known as deduplication. Deduplication comprises three parts: duplicate detection, duplicate verification, and duplicate resolution.

- **Duplicate detection** refers to the process of identifying duplicates in the CR. Two or more records are designated as possible duplicates if they are determined to map to the same real-world individual. Duplicates may be detected by a user during the normal querying process of the CR, or automatically by the CR in an automated background process that runs periodically. Both the deterministic and probabilistic approaches described under identity resolution may be used for duplicate detection as well.
- **Duplicate verification**, on the other hand, refers to the process of checking whether a detected duplicate represents an erroneous multiple entry for the same client or is simply a false positive
- **Duplicate resolution** refers to the process of merging verified duplicates to create a single client identity in the Kenya Master Health Client Registry (KMHCR) while the process of identifying duplicates is automated, the duplicate resolution is deferred to a human actor.

1.6.6 Merging Patient Records

Duplicates flagged must be presented to registration personnel for resolution. It is the responsibility of the registration personnel to verify the correctness of the flagged duplicates, by referencing additional sources of information. False duplicates may be ignored, and the duplication identification algorithm can be asked not to flag the false duplicates in the future.

Merging patient identities has potentially serious results. If performed erroneously, it can lead to adverse outcomes for patients. For example, a patient can be denied life-saving treatment based on allergies that they do not have, but which have been recorded as having because of an erroneous merger with another patient's data. For this reason, strict protocols will be developed to govern the process. Also, as already mentioned, the UPI system must be designed to minimize the chances of the same patient being entered in the system more than once.

1.7 Non-Functional Requirements

1.7.1 Interoperability

Interoperability refers to the ability of different information systems to integrate and cooperatively exchange data in a coordinated manner. The UPI system will comprise multiple components that provide specific services to each other. As such, each participating application will need to provide an interoperability interface to support communication with other systems. Specifically, participating applications will be required to support RESTful web services and to package their payloads in standard Health Information Exchange formats, principally Health Level

7 (HL7) and Fast Healthcare Interoperability Resources (FHIR). The interoperability platforms offer integration patterns and components to support interoperability across the Kenya health information system echo system.

1.7.2 Reliability

Reliability refers to the probability that a system performs correctly and follows the defined performance specifications. Multiple clinical systems, such as the EMR systems and the SHR, will rely on the KMPR for identity management on an ongoing basis. Consequently, policies and provisions must be made to support maximum uptime and performance of these shared resources as well as the interoperability platforms that will be responsible for facilitating communication between them. Proposed design approaches to maximize reliability include database replication for redundancy, load balancing, and routine monitoring of system logs to identify and resolve technical errors and performance bottlenecks before they manifest themselves to system users.

1.7.3 Availability

Availability is the likelihood that a given system will be available to users at any given time. The KMPR shall promote the achievement of availability by implementing redundancy measures to decrease the likelihood that the system is not available to users on demand.

1.7.4 Flexibility

Flexibility refers to the ability of the system or program to be used for multiple purposes, rather than a single function to accommodate a certain amount of variation regarding the requirements of the supported business process. It can also be regarded as a response capability to predicted or unforeseen changes in the organization or environment. Flexibility is the capability to adapt to new, different, or changing requirements.

There are two main dimensions of flexibility that include structural and process flexibility. Structural flexibility denotes characteristics of information systems themselves, such as modularity, acceptance of change, or consistency. Process flexibility is described as the ability of organizations to adjust information systems to new situations. This includes the skills necessary for adaptation such as programming, change management, or coordination of activities.

1.7.5 Extensibility

Extensibility is a measure of the ability to extend a system and the level of effort required to implement this extension. Platform extensibility means that a user can extend a software platform and add more functionality to the system for enhancements without impairing existing system functions. Extensibility adds to the base functionality, thereby offering new capabilities and outputs.

1.7.6 Consistency

Consistency is the requirement that any given database transaction must change affected data only in allowed ways. Any data written to the database must be valid according to all defined rules, including constraints, cascades, triggers, and any combination thereof.

Consistency is the requirement that any given database transaction must change affected data only in allowed ways. Any data written in the database must be valid according to all defined rules, including constraints, cascades, triggers, and any combination thereof.

1.7.7 Scalability

Scalability refers to the ability of a system to handle increasing workloads. KMPR will be responsible for servicing an increasing number of EHR systems, such as EMRs, as more health facilities participate in the UPI system. For this reason, appropriate provisions must be made to scale these services in terms of both hardware resources and application-level optimizations.

1.7.8 Maintainability

Maintainability refers to the ease and speed with which a system can be restored to operational status after a failure occurs or a modification is requested. As such, maintainability is a major enabler of reliability, as it has a direct impact on system uptime and performance. The specific proposed strategies for promoting the maintainability of the UPI system include clear and concise code, separation of concerns, modularization, unit testing, continuous integration, technical documentation, and general conformance to software design and development best practices.

1.7.9 Usability

Usability relates to the effectiveness, efficiency, and satisfaction associated with using a system. In other words, users should be able to achieve their objectives with minimum effort while enjoying the overall experience of interacting with the system. In practice, this means easy-to-use and intuitive user interfaces that blend into the users' daily workflow. It also involves using commonly understood terminology; showing helpful error messages (with recovery instructions where applicable); specifying meaningful defaults for common data entry fields and minimizing or eliminating distracting and non-essential features.

1.7.10 Security

Security refers to the various methodologies used to keep confidential information safe from unauthorized access, theft, corruption, and other types of damage. Clinical data and identity are inherently confidential and therefore, the UPI system will adhere to the most stringent industry standard information security practices. These include strong password protection for individual user accounts (with salting and hashing to prevent theft); Public Key Infrastructure (PKI) to limit administrator access to authorized devices only; Transport Layer Security (TLS) to encrypt data in transit and prevent eavesdropping attacks; software and hardware firewalls; intrusion monitoring; regular software updates and staff training and sensitization on data security and confidentiality best practices.

SECTION 2: IMPLEMENTATION STRATEGY OF UNIQUE PATIENT IDENTIFICATION

The implementation and operationalization of the UPI will involve the development and deployment of four critical components namely, the KMPR, the SHR, the Interoperability Platform, and Point of Care Systems (Principally the DHP but also other client-facing systems such as EHRs and CHIS). The KMPR will serve as the main database containing authoritative data on patient identities across the country. The SHR system, on the other hand, will be used to collate individual health records from the DHP and other Point of Care systems in a centralized database to share data to support continuity of care and improve the quality of clinical decision-making. All Point of Care systems including the DHP will interface with both the KMPR and the SHR through the Interoperability Platform to access patient identity and health record exchange functions respectively.

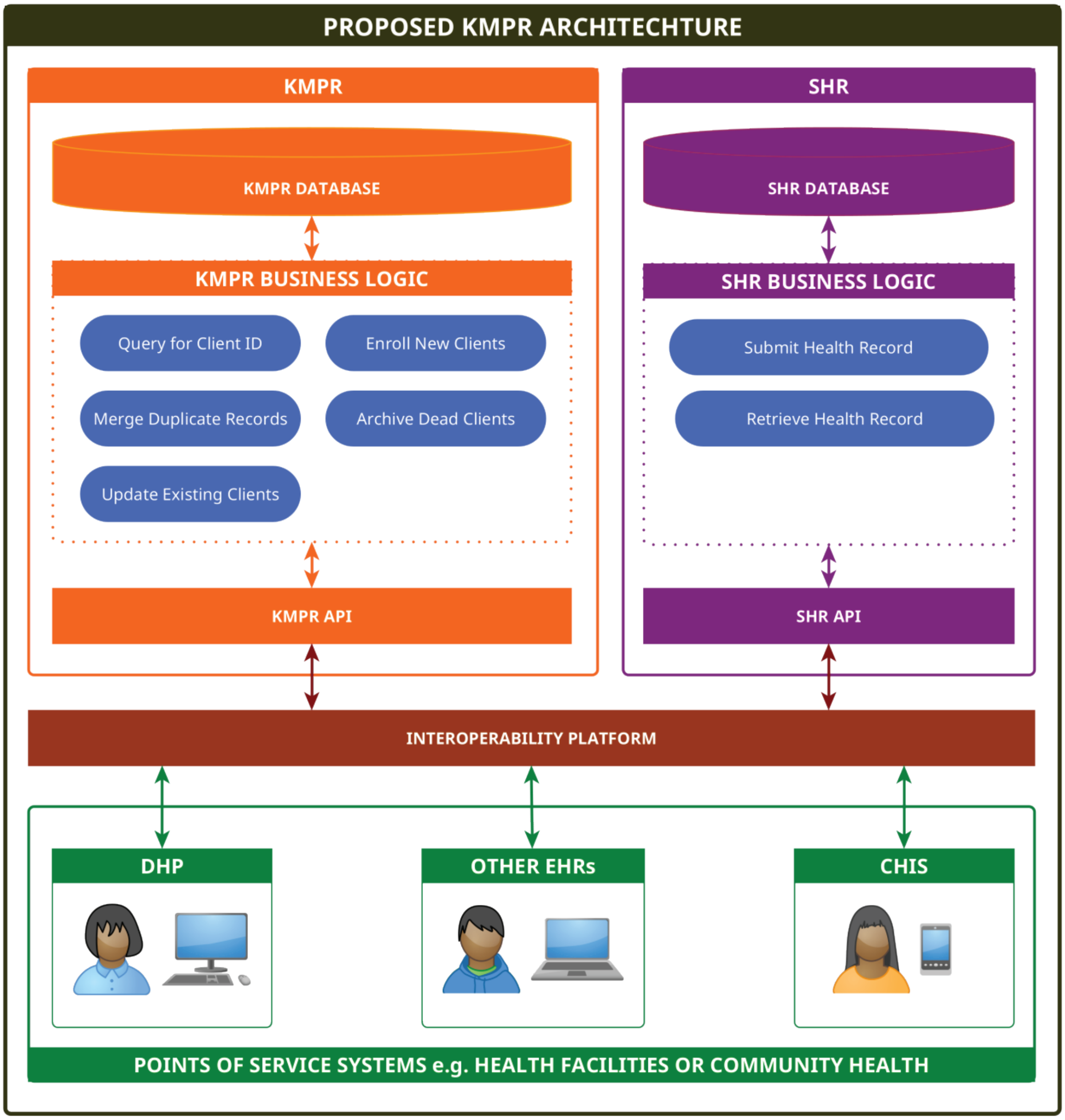

Figure 1- Conceptual Model of the Components and Interactions of the UPI System

2.1 Components

Enterprise level system components comprise the KMPR, SHRs, and the Interoperability Platform while the facility-based digital solution comprises point of care systems, including the DHP. Figure 1 presents the components of the enterprise-level system and linkages.

- The KMPR serves as the source of truth for patient identity and management in healthcare services Point of Care Systems, as digital versions of a patient's paper chart, are a real-time, patient-centered records system that makes information available instantly and securely to authorized users
- The SHR facilitates sharing of clinical information between HIS to enable better patient care thus improving health outcomes
- The interoperability platform will be responsible for message transmission between the other three components, including providing common services such as routing, queuing, and transport layer security across the network

2.1.1 Kenya Master Patient Registry

The KMPR is a central repository (database) that contains personal attributes of patients such as name, gender, date of birth, telephone number, and physical address, as well as government issued identifiers like their National ID, Huduma Namba, passport number, driver's license number, NHIF Number, telephone numbers, etc. Biometric data may also be accommodated, as well as local identifiers issued at various service delivery points within the health facility. All available identity information will be mapped to a UPI that refers to a single patient in the registry.

This enables the registry to cleanly integrate with other available identifier systems, including any that may be created in the future. The necessary logic for deterministic and probabilistic matching should be implemented as described earlier in the document. An interface will be provided for EHR systems to query and update the KMPR. The KMPR serves as the primary identity database for patients seeking health services and should be hosted centrally at the national level. EHR systems intending to resolve patient identities will issue a search query in a standardized format (e.g., the demographics query to the KMPR) and a result will be returned in real-time.

In the case of probabilistic identity resolution searches, more than one match may be returned, along with an associated score indicating the quality of the match. Facilities without an EHR will register patients through facility issued mobile devices into the national KMPR. They will have the functionality to query UPIs from the national KMPR. The identification process for a patient at service delivery points should include searching the local instance of EMR or the national KMPR to match identifiers and verify the information. Depending on the identifier's scope and level of use, the search processes can range from a single provider organization to KMPR.

2.1.2 Local Patient Registry

The Local Patient Registry (LPR) is a deployment of the KMPR hosted at health facilities to ensure optimal performance of facility EMRs when querying to resolve patient identities. The EMR/EHR systems of the facility will query the LPR, and the results are expected in real-time. When a match is not found in the LPR, this is extended to KMPR. In the case of probabilistic search, more than one match may be returned, along with an associated score indicating the quality of the match. When there is no match after the extended search in the KMPR, the registration of a new patient into the system is initiated. Figure 2 represents the process.

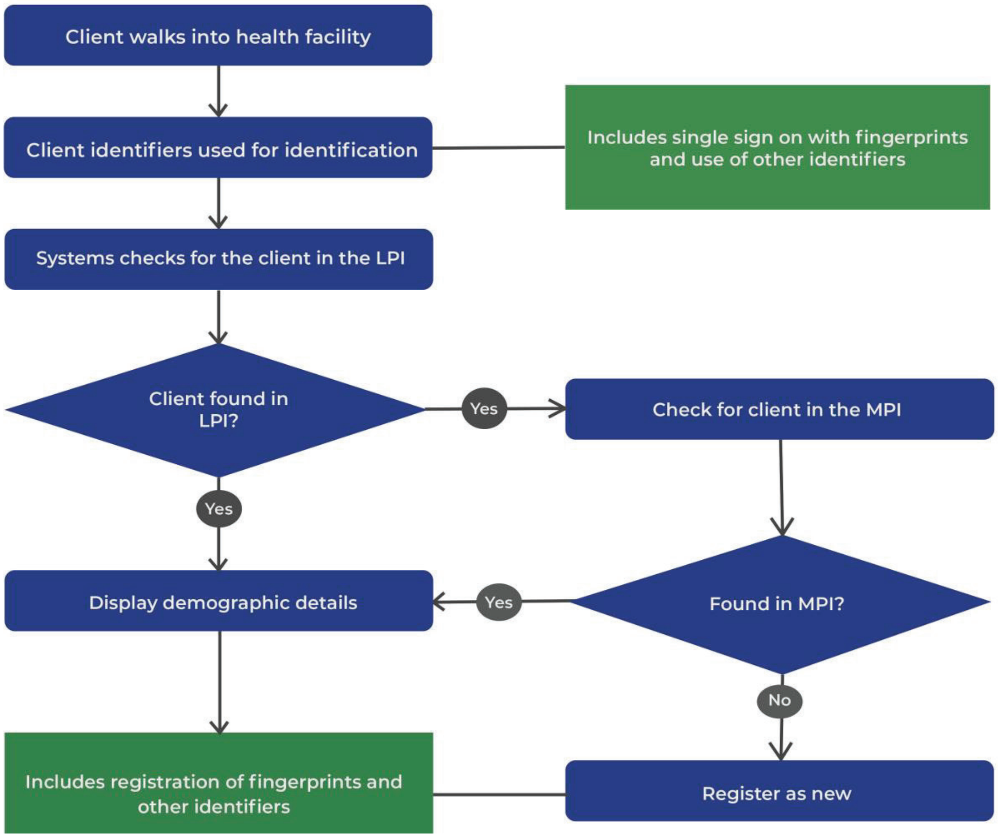
Client walks into health facility
Client identifiers used for identification
Includes single sign on with fingerprints and use of other identifiers
Systems checks for the client in the LPI
Client found in LPI?
Yes
Check for client in the MPI
Yes
Display demographic details
Yes
Found in MPI?
No
Includes registration of fingerprints and other identifiers
Register as new

Figure 2- Patient Registration and Verification Flow

2.1.3 Electronic Health Record

An EHR refers to an electronic record of a patient and may contain information on demographic data, clinical data (such as past consultations, lab results, diagnosis, and treatment), scheduling, insurance, and billing information. This information is accessed by EHR systems, by resolving the identification of a patient. Healthcare professionals and providers use software systems to manage patient health records. These systems ensure security, validate information for completeness, and prompt for additional information where applicable. One key parameter of an EHR is the UPI, which is the link that ensures that the EHR information is about a specific patient. Examples of these digital EHR systems include: EMR systems, laboratory information systems (LIS), pharmacy information system (PIS), and community health information systems (CHIS).

During a patient visit to a facility the output generated by an EMR may contain the diagnosis, treatment, and other details regarding the visit. EMR systems are used to identify and record information related to the patient's visit. A client's health record may be spread out across multiple EMR systems, such as when a client is seen in multiple facilities or several departments in the same facility. On completion of the visit, the EMR information is subsequently used to update the EHR of the patient.

EMRs will be able to resolve client identities correctly and consistently against the LPR/KMPR as well as register new clients and update details of existing clients. EHRs will be able to query an SHR data repository, as well as update it with new client data on an ongoing basis. The specific processes for achieving this are described in the workflow section of this document.

2.1.4 Shared Health Records

An SHR system is a centralized database repository that facilitates the sharing of information between EHR systems to improve patient management and generate vital public health data for evidence-based decision making. The proposed SHR system will be implemented as a document store capable of being updated with new documents and serving existing documents upon request. The documents are clinical encounter records generated and submitted by her systems and packaged in a standardized format.

SHRs are the minimum data elements or variables of the health data required for patient management during a visit to a health facility. The healthcare providers will rely on the SHR to obtain up-to-date information on past consultations, diagnoses, investigations, treatment, as well as allergies and other information useful for providing optimal clinical care. These minimum patients' data elements are collated from various digital health solutions and updated with the data from the most recent health facility visit where the healthcare services were sought.

The SHR will provide a public application programming interface (API) through which EHRs can securely interact with the system for updates and queries supporting standard health information exchange formats, such as HL7 and FHIR.

2.1.5 Interoperability Platform

An interoperability platform is a communication system between software applications. It offers the necessary components to support information exchange across digital health systems. It provides flexible, higher-level communication protocols between applications by handling low-level communication details such as message routing, queuing, and security. The interoperability platform is at two levels—central and local interoperability platforms.

- The **central interoperability platform** is responsible for facilitating communication between the other 3 components of the enterprise ecosystem namely, the KMPR, the SHR system and digital health systems, and the local interoperability platform at the health facility
- The **local interoperability platform** will be responsible for routing messages between digital health systems within a health facility

Messages that cannot be delivered within the facility are forwarded to the central interoperability platform for onward transmission to the KMPR or SHR. Responses from any of the central systems (e.g., Master Patient Index (MPI) or SHR) coming through the central interoperability platform will be delivered to the local interoperability platform for final transmission to the originating EHR system. Specific workflow details are covered in Section 2.2.

2.2 Workflows

This section describes the workflows for managing UPI through the components described in 2.1 Components. It covers:

- Patient registration
- Unique identifier generation and assignment
- Updating Patient details on the KMPR
- Querying the SHR
- Updating the SHR

2.2.1 Preloading Data from Existing Databases

Patient identity data will be preloaded from existing databases during the initial deployment of the KMPR. Through an Extract Transform and Load (ETL) process, the KMPR will access data from existing databases such as ChanjoKE, subject to the necessary approvals and compliance with the existing laws and import the same into the KMPR database. Appropriate data validation mechanisms such as checks for completeness and duplication will be configured within the system to ensure that only clean records are imported into the patient registry. During the data import process, a UUID will be generated and assigned to each patient record to facilitate future patient searching and identification via the KMPR. The registry will then continuously grow and expand through routine updates and enrollment of new patients at various health service delivery points.

2.2.2 Querying the Patient Registry

Searching for patients in the KMPR is the primary function of the UPI system. It serves as the first point of interaction between the patient, care provider, and KMPR. A patient search is initiated using government issued identification documents or other unique identifiers such as patient names, national identification cards, Huduma numbers, birth certificates, and mobile phone number. Where a point of health care does not have the required infrastructure, an API or mobile app will be availed to enable users to access the KMPR. If the patient does not provide any usable deterministic attributes, a probabilistic search is used. In this case, the patient provides a select set of probabilistic attributes such as their name(s), sex, date of birth, physical address, and mother's maiden name. If a match is returned, it is verified by gathering additional information from the patient to corroborate the search information returned from the registry.

The patient identification search request is executed at both KMPR and the provision database LPR and routed through the local and central interoperability platforms. The search must be done in real time and should not be queued. Ideally, both indices should be coordinated and should return equivalent results. A positive match completes the identification process and delivers the patient's attributes along with their UPI to the querying EHR. In the absence of a match, the care provider proceeds to the workflow for updating the patient registry.

2.2.3 Creating New Patients

The creation of a new patient is performed when the patient search workflow returns zero positive matches, and the care provider is satisfied that the patient has not been previously entered in the KMPR. In this case, all available personal attributes supported by the registry are collected and entered at the local patient registry. The Kenya Master Patient Registry is updated after the record is successfully saved at the LPR.

2.2.4 Updating Existing Patients

Updating the KMPR registry modifies the details of an existing patient data or the creation of a new patient. The circumstances necessitating updates are either the correction of wrong or out-of-date information (e.g., typo error or a name change due to marital status) or any additional missing attributes that were not included when the patient record was first created. The KMPR is updated after the updated record is successfully saved at the LPR.

2.2.5 Merging Duplicate Patients

Merging refers to the process of combining two or more patient records. The two patient records are determined to belong to the same patient in the KMPR but are entered as different clients, each with a different UUID. The result of the merger should be one patient record in the KMPR indexed by one UUID. Generally, the following three possibilities could lead to duplicate client records in the patient records:

- **Intentional misrepresentation**: A patient intentionally misrepresents their identity during registration and as a result is enrolled under multiple identities. This possibility can be mitigated by requiring official proof of identity during enrollment
- **Poor querying technique**: Registration personnel fail to conduct a thorough client search and identity resolution before registration. This possibility can be mitigated by proper user training and through the automated pre-registration search
- **Technical hitches**: Registration personnel fail to connect to the patient records due to technical challenges and therefore perform a provisional registration locally. This possibility can be mitigated through enhanced patient availability and prompt technical support.

2.2.6 Archiving a Patient

Once a duplicate occurs in the patient records, it must be identified, verified, and resolved. Duplicate identification refers to the process of noticing or flagging suspected duplicates. Duplicate verification, on the other hand, refers to the process of checking whether a detected duplicate represents erroneous multiple entries for the same client. Duplicates may be detected manually at the point of service during a routine patient record query or automatically by an algorithm that runs periodic duplicate checks on the patient registry. The process for detecting duplicates involves an equivalence analysis between two or more client identity records with the goal of generating a similarity score. Records with a high enough similarity score are flagged as possible duplicates awaiting verification and resolution.

SECTION 3: LEADERSHIP AND GOVERNANCE FOR UPI IMPLEMENTATION

Leadership and Governance ensures that strategy policy frameworks exist and are combined with effective oversight, coalition building, regulation, keen attention to system design and accountability. Accountability is an intrinsic aspect of governance that concerns itself with the management of relationships between various stakeholders in health, including individuals, firms, and both levels of governments (national and county), non-governmental organizations (NGOs), and other entities that have the responsibility to finance, monitor, deliver and use the services.

The UPI implementation will be overseen by the office of the Director General of the Ministry of Health (MOH) through the Directorate of Health Policy, Research, and Monitoring & Evaluation (M&E). At the county level, UPI implementation will be undertaken through the office of the County Director for Health Services/Department of Health responsible for public health.

The UPI framework implementation and monitoring will be achieved through the Health Information Inter-Agency Coordinating Committee (HI-ICC) at the national level and the partners' forums at the county level. At the national level, the Department of Health Sector M&E and Informatics of the MOH will be the custodian of the framework and at the county level it will be under the department responsible for health. This will be guided by oversight structures and processes as stipulated by the Intergovernmental Relations Act No. 2 of 2012 and operation manual from the Health Sector Intergovernmental Relations Forum of 2018.

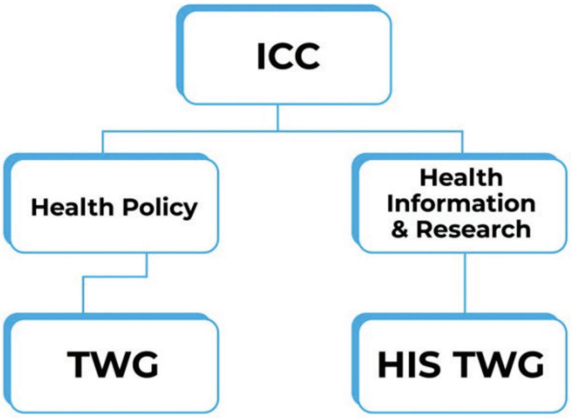

Figure 3- The HIS ICC and the HIS TWG

The implementation is further anchored on the Data Protection Act, 2019, the Health Act, 2017, Kenya National eHealth Policy 2016-2030, Health Sector M&E framework 2018-2023, NIIMS legislations (Registration of Persons Regulation 2020, Data Protection Regulations 2021, the Huduma Namba Regulations 2020) and any other relevant laws. The key drivers for successful implementation of this protocol shall revolve across shared responsibilities, accountability, and interdependence.

The leadership of the UPI framework shall be provided both at the national and county levels. The national HIS secretariat will facilitate communication between the national and county levels, identify key HIS issues, prepare agenda items for the HI-ICC, and ensure that action points arising from HI-ICC are adequately addressed. It will be chaired by the Director-General through delegated authority to the Head of Directorate, while at the county level it shall be chaired by the County Director of Health.

3.1 Roles and Responsibilities

3.1.1 National Health Information, Inter-agency Coordinating Committee

The HI-ICC will be responsible for coordinating UPI implementation, collaboration, and consultation between the various stakeholders. To effectively ensure a successful implementation of UPI at all levels, the UPI implementation will be undertaken under the relevant technical working groups (TWGs) during implementation. The HI-ICC will provide a forum for joint planning, coordination, and monitoring of specific investments during UPI framework implementation.

The committee will be chaired by the Director-General through delegated authority to the Head of Directorate and will be co-chaired by the Chair of the corresponding Health Sector Intergovernmental Consultative Forum (HSIGCF), Thematic Technical Committees (TTC) and a designated Development Partner (DP) representative.

The HIS-ICC will meet at least monthly or as frequently as the committees determine necessary and will report to the higher-level committees through the Partnership Secretariat. HIS -ICC members will include:

- MOH Heads of Departments, Divisions, Units, and programs
- County Directors of Health (CDOH) representatives
- Representatives from relevant health-related and enabling ministries
- Technical representatives from Development Partners and UN Technical Agencies
- Implementing Partners for related donor-funded projects and programs
- Health NGO Network (HENNET) members representing NGOs and civil-society organizations (CSOs)
- Faith-Based Organizations (FBOs):
    - Christian Health Association of Kenya (CHAK)
    - KCCB Catholic Health Commission, and Supreme Council for Kenya (SUPKEM).
- Private sector partners represented by the Kenya Healthcare Federation (KHF)
- Other partners may be co-opted as needed to inform discussions and decision-making

3.1.2 Functions of HIS–ICC

The main functions of the HI-ICC are to:

- Bring all key sub-sector partners together for joint planning, oversight, and decision-making
- Enable partners to become jointly responsible for planning, monitoring, reviewing, and reporting
- Hold all sector partners jointly accountable for achieving results
- Reduce the number of separate meetings with individual partners
- Enable harmonization of inputs and better coordination of investments in the sector partnership for more effective use of all available resources to reduce duplication of efforts and critical gaps
- Facilitate coordinated technical assistance and support for priority actions. The HI-ICC will form TWGs, task teams or task forces as needed to address specific priority issues and areas of focus
- Seek and integrate patient interest in implementation

3.1.3 Duties and Responsibilities

- Overall custodial and coordination duties of the implementation of the UPI framework
- Mobilize resources and financing for implementation of core UPI components
- Implementation of the UPI framework
- Coordination, evaluation, and periodic review of the UPI implementation framework
- Maintain centralized database for the KMHCR
- Capacity building of county governments
- Technical assistance to counties
- Monitor compliance of UPI framework
- Progress and performance evaluation using UPI framework
- Coordination mechanisms for the health-sector UPI working groups including partners supporting MOH at the national level
- Assurance for stakeholder's implementation of UPI framework at all levels
- Adequate consultations and participation of both levels of government in the UPI implementation process
- Sufficient resources are available to ensure implementation of the UPI framework
- Strict adherence to and enforcement of the framework
- Resource Mobilization and financing for implementation of UPI
- Participate in the implementation of UPI framework within county jurisdictions
- Mobilize and allocate resources for the implementation and monitoring of the UPI framework at health-facility level
- Review and jointly monitor UPI framework compliance at the county level periodically
- Enforce facility level adherence to the UPI implementation process

3.1.4 County-Level Coordination Structures

Counties are advised to establish county UPI coordination structures best suited to their needs and may take guidance from the health sector partnership structures outlined. The main purpose will be to ensure that CDOHs, County Officers for Health (COHs) and County Executive Committee Members for Health (CECMs-Health) are fully aware of and informed on implementation of the UPI.

It is assumed that counties have established a county health sector coordinating committee or forum that brings together all actors in health at the county level on a regular basis to discuss and agree on prominent issues affecting the county, and to coordinate and harmonize all inputs and investments for health at the county level. The forum would ideally meet on a quarterly basis. Membership should include state actors at county level e.g., CECM-Health, COH, CDOH, County Health Management Teams (CHMTs), heads of hospitals, sub-county officers, health-related departments (water, education, agriculture); and non-state actors FBO service providers, NGOs, implementing partners, key CSOs, etc.

The County Coordinating Committee (CCC) will be responsible for coordinating UPI implementation, collaboration, and consultation between the various stakeholders at the county level. To effectively ensure a successful implementation of UPI, the CCC is tasked with providing technical guidance to all stakeholders.

The CCC will set the timelines for implementation of UPI in the county and hold periodic review meetings. Figure 4 shows the UPI governance structure.

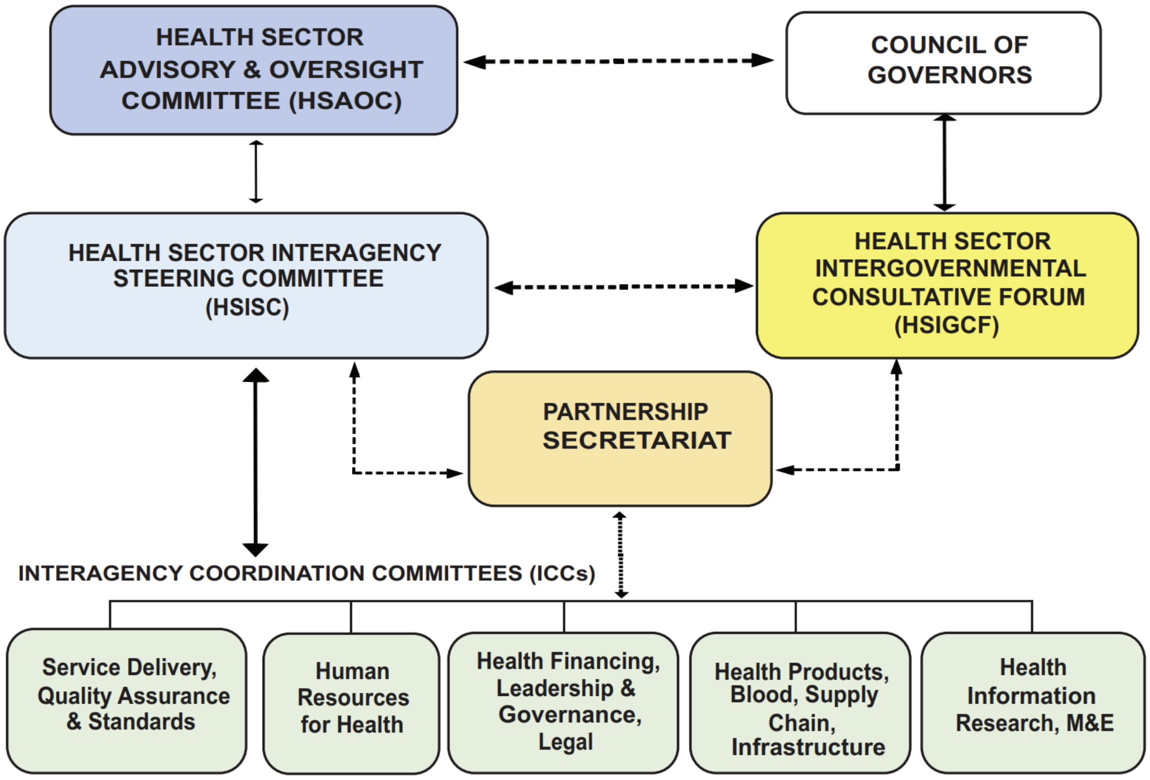
HEALTH SECTOR ADVISORY & OVERSIGHT COMMITTEE (HSAOC)
COUNCIL OF GOVERNORS
HEALTH SECTOR INTERAGENCY STEERING COMMITTEE (HSISC)
HEALTH SECTOR INTERGOVERNMENTAL CONSULTATIVE FORUM (HSIGCF)
PARTNERSHIP SECRETARIAT
INTERAGENCY COORDINATION COMMITTEES (ICCs)
Service Delivery, Quality Assurance & Standards
Human Resources for Health
Health Financing, Leadership & Governance, Legal
Health Products, Blood, Supply Chain, Infrastructure
Health Information Research, M&E

Figure 4 - UPI governance structure (Adapted from Health Sector Partnership Coordination Framework 2018 -2030)

SECTION 4: MONITORING AND EVALUATION

4.1 Components of UPI M&E system

The UPI framework is anchored on the 12 main components of any functional system, which define the Organizing Framework for a Functional National UPI M&E System (UNAIDS, 2008). Consequently, this UPI also focuses on using the 12 components of M&E System Strengthening Tool (Geneva: UNAIDS, 2009) to ensure a comprehensive and successful assessment.

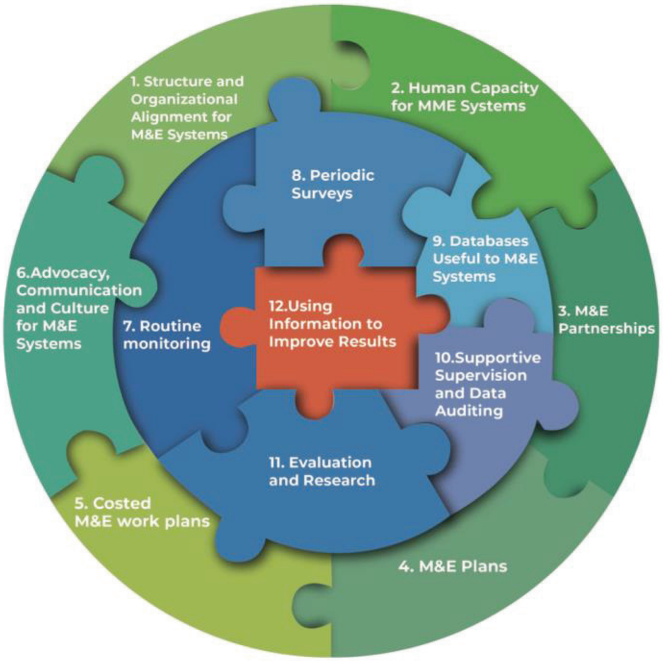
1. Structure and Organizational Alignment for M&E Systems
2. Human Capacity for MME Systems
3. M&E Partnerships
4. M&E Plans
5. Costed M&E work plans
6.Advocacy, Communication and Culture for M&E Systems
7. Routine monitoring
8. Periodic Surveys
9. Databases Useful to M&E Systems
10.Supportive Supervision and Data Auditing
11. Evaluation and Research
12.Using Information to Improve Results

Figure 5 - UPI M&E Components (Adapted from Gorgens M. and Kusek J. Z. (2010). Making Monitoring and Evaluation Systems work: A Capacity Development Toolkit.)

The 12 components provide an acceptable standard for the UPI to function effectively. The UPI M&E components in figure 5, represent the UPI framework monitoring plan, which is aligned to the existing MOH sector coordination and collaboration mechanism and the above documented HI-ICC structure.

Components 1 through 6 relate to health sector stakeholders, partnerships, and planning support for data production and use. These components relate to the existing enabling environment for the health sector coordination and collaboration mechanism to create a functional and dependable M&E system. The components present coordination procedures that the HI-ICC will utilize to plan, budget, and cost a well-functioning UPI framework M&E system.

Components 7,8,10, and 11 relate to the data management processes that involve the collection, collation, capture, and verification of types of M&E data. These components generate data essential to the M&E system, through UPI data generation, analysis, and dissemination for decision and policy support. Component 12 focuses on the capability and capacity of the UPI M&E system to consistently create health data and information as a means of informing and empowering decision-making across all levels.

4.2 UPI Implementation Roadmap

The implementation of Kenya Health Sector UPI framework will involve periodic collection and analysis of data to monitor and evaluate the progress towards the realization of intended objectives. The process of implementing this framework will begin by conducting leadership consensus and stakeholder engagement meetings at the strategic level. The purpose of this will be to create awareness and advocacy for the leadership and stakeholders on the importance and relevance of correct patient identification in a positive fashion that also respects concerns for privacy share and discuss UPI framework for adoption. This will be followed by the configuration of UPI in the national data center and in health facilities for real time use.

Capacity building for national departments, divisions, programs/projects will be conducted to enable usage of UPI and across service delivery points. In addition, Counties and health stakeholders will be trained on UPI so as to fast-track adoption and implementation.

Continuous monitoring will be carried out to measure adoption, uptake, and usability of UPI. Similarly, continued technical support will be provided to mentor users and resolve identified challenges during implementation. Lessons learned will be shared in appropriate forums.

4.3 Security

Security and access control are critical in sharing personal and health data. Healthcare data has been classified as 'sensitive data' in the Data Protection Act, 2019. Consequently, assessment of data security controls by health data entities through conducting risk assessment, and implementing risk management programs to address any vulnerabilities that are identified by any entity that generates, stores, shares or transmits health data is critical. The government of Kenya has put in place measures to protect health data at all levels and will continuously monitor any attempts to circumvent these measures. Part of the measures include development of a National Health Data Warehouse where all health data is stored. Additional measures are articulated in the Data Governance Framework 2022 -2025.

Table 4 shows the Access Control Components that will be used to ensure continuous security of data collected.

Table 4 - Access Control Components and Uses

Control	Used for
Consent Form	Patients to give permission to form part of the registry patients will be educated about UPI.
Role-based Access Control (RBAC)	User accounts are associated with roles for all access to UPI software, for example clinic receptionist, medical records clerk, etc.
Encrypted Passwords	All passwords are stored with non-reversible and strong encryption.
Virtual Private Network (VPN)	Where a secure link cannot be established with the MPI, the UPI infrastructure will use a VPN to secure messages in transit.

Secure Sockets Layer (SSL)	Strong encryption is used to send messages through the web using HTTPS (HyperText Transfer Protocol, Secure). The UPI must encrypt all messages on the VPN using SSL.
Public Key Infrastructure (PKI)	For a national rollout, this establishes a web of trust. Messages can be signed to positively authenticate the sender and encrypted so that only the intended recipient can read them.

PKI is used when sending a message from one clinic to another. Each facility has a private key that only the facility knows and a corresponding public key that is freely known to all. A message may be signed using a sending facility's private key and anyone may use the sending facility's public key to verify (authenticate) that the message was signed by that facility. Also, a message may be encrypted using a designated facility's public key and only the destination facility may decrypt the message using its private key. These two techniques may be used together. This results in a message that can only be read by the destination clinic and could only have been sent by the source clinic.

PART II: KENYA PATIENT REGISTRY REQUIREMENTS SPECIFICATIONS

INTRODUCTION TO SPECIFICATIONS

The Government of Kenya is committed to creating the necessary laws, policies, and standards to achieve quality, accessible, and affordable health care for its citizens. This is in line with the stipulations contained in the Constitution of Kenya, the United Nations Sustainable Development Goals (SDGs), Vision 2030 and other treaties and covenants that provide for citizens' right to health. Indeed, health and wellbeing are central to the President's Big Four Agenda, a development blueprint which includes, among other things, the achievement of UHC for all Kenyan citizens by the year 2022.

Accurate and timely data is critical to help guide the deployment of resources for UHC as well as monitor its implementation, inform public health response, and optimize healthcare delivery for individual clients. However, paper-based methods of data collection and management have proven to be inadequate for meeting this growing demand for information. As a result, there has been a gradual shift towards the use of Information and Communications Technology (ICT) to address the need for timely and accurate data. Indeed, the MOH recognizes ICT as a key enabler towards the achievement of UHC.

Currently, there exists multiple innovations in HIS in Kenya. These include EMR systems, LIS, PIS, Hospital Management Information Systems (HMIS), the Logistics Management Information System (LMIS), the Kenya Health Information System (KHIS), the Kenya Health and Research Observatory (KHRO), among others. Despite these interventions, there continues to be a gap in the capacity for these systems to work together in a cohesive and interoperable manner. This makes it difficult to collate and share information, thereby undermining the ability to make maximum use of the available data to inform client-level and public health decision making.

The MOH, through the deployment of the Digital Health Platform (DHP), envisages a comprehensive HIS comprising specialized point-of-care modules, centralized applications, and an interoperability platform to orchestrate communication and data sharing between these systems. Specialized point-of-care modules include client registration, consultation, laboratory, imaging, pharmacy, client referral, mortuary management, and even billing and insurance claims processing. Shared centralized applications include KHIS, Kenya Master Health Facility List (KMHFL), LMIS, Integrated Human Resource Information System (IHRIS), SHR system, among others.

In practice, the functionality contemplated in the DHP may be delivered as part of one or more information systems. For example, in a health facility with a fully-fledged HMIS, client consultation; laboratory and radiology investigations; drug prescription and dispensing; as well as billing and payment processing can all be managed under one application. On the other hand, in a less-endowed health facility, clinical consultation may be processed within an EMR system while laboratory investigations and drug dispensing are processed in a separate LIS and PIS respectively, i.e., system interoperability within the same health facility. A more sophisticated use case might involve a client referral from one health facility to another, i.e., system interoperability between health facilities. In this case, the referring facility generates a client's clinical summary and sends it to the referral facility for follow-up. Beyond this, health facilities can also submit de-identified client data to a central SHR system to facilitate information sharing across physical locations. This has the double benefit of enhancing individual client care while providing invaluable case-based data to generate accurate service statistics for planning and decision making.

In order to facilitate communication and data sharing between disparate information systems as described, it is necessary for each participating application to share some common semantics. These semantics are comprehensively addressed in the Health Data Dictionary. For example, a prescription raised from within an EMR for fulfillment in a PIS must be consistently and reliably associated with the same client on both applications. Similarly, a referral raised from an EMR in one health facility must be linked to the same client at the destination health facility. Instructively, mismatches in client identities in interoperability workflows like these can lead to potentially harmful results. For example, a client may be issued with medication belonging to someone else or be treated based on allergies or medical history associated with another client. At a public health level, service statistics may be unintentionally over reported if the same client is counted more than once or underreported if multiple clients are misidentified as one patient. This can lead to poor program planning, sub-optimal use of resources and ultimately, adverse health outcomes.

The correct and unambiguous identification of individuals seeking healthcare, therefore, is a critical feature of any safe and effective interoperability environment. In order to meet this requirement, individual information systems cannot maintain their own versions of client identity data as the same client risks assuming multiple identities under each application. Instead, all systems must rely on a shared and authoritative only source of truth against which client identities are resolved. This only source of truth is referred to as a CR. The KPR is an electronic database that holds demographic information on every client who receives healthcare services within a certain jurisdiction and aims to accurately match and link records by uniquely identifying individuals. This document defines the functional specifications for the KPR which is designed to support a variety of interoperability use cases within the health system.

PURPOSE

This Software Requirements Specification (SRS) document covers the features of the KPR as well as the context within which the system will be implemented. It includes a detailed description of the users of the system and their characteristics, external interface requirements, expected system functionality, workflows, and non-functional specifications. The goal of this SRS is to provide managers, developers, implementers, and users of the KPR with a clear and detailed description of the product. This will help facilitate project planning, resource mobilization, application development and the pre-deployment preparation necessary to take full advantage of the KPR.

SECTION 5: OVERALL DESCRIPTION

5.1 Product Scope

This SRS relates exclusively to the functionality provided by the KPR as the authoritative single source of truth for client identification in the health sector. The KPR is a general-purpose shared resource dedicated to servicing client identity resolution requests from a variety of third-party applications. This document identifies and provides examples of such third-party applications and the associated use cases. However, it is not within the scope of this document to specify the functionality of those third-party systems beyond what is necessary to describe their interaction with the CR.

5.2 Product Perspective

The KPR is envisaged as a component of the broader Digital Health Platform (DHP). For this reason, the system must be designed with the other components of the DHP in mind. This includes not just existing applications such as EMRs and the KHIS, but also those that will be developed in the future like the SHR system. All interoperability within the DHP will be facilitated through a general-purpose interoperability platform. The CR, therefore, will be expected to support the same communication protocols as other applications participating in the overall DHP interoperability framework.

In addition to the DHP, the KPR is also expected to be loosely integrated with the NIIMS, also popularly known as the Huduma System. Specifically, the KPR will include the NIIMS ID (Huduma Namba) as one of the unique identifiers by which patients will be identified.

5.3 Product Functions

The KPR shall serve as an accurate and up-to-date electronic database containing the demographic information on every client who receives healthcare services in Kenya. It shall also offer the capability to service client resolution queries from duly authenticated third-party applications according to laid down communication protocols. In order to fulfill these functions, the KPR shall provide the functionality below:

- **Querying for client identity:** The KPR shall provide an interface through which authorized users can query the database for identity resolution based on known client attributes. The system shall support deterministic, probabilistic, and biometric matching algorithms to maximize the chances of correct unique client identification.
- **Enrolling new clients:** The KPR shall provide an interface through which authorized users can submit data on new clients for inclusion in the registry. Additionally, the system will have mechanisms to minimize accidental duplicates and other errors during the enrollment process.
- **Updating existing clients:** The KPR shall provide an interface through which authorized users can update data on existing clients to add new information, correct errors or accommodate legitimate changes in personal details. This will ensure that the system is always as up-to-date as possible.
- **Merging duplicate clients:** The KPR shall define and support clear protocols for the detection, verification and merging of duplicate client records. This will serve to maintain database health and maximize the chances of

correct and unambiguous client identification.

- **Archiving dead clients:** The KPR shall provide an interface through which authorized users can designate deceased clients for archival. This will physically or logically migrate the affected client's identity data to a less frequently accessed part of the KPR and therefore improve the system's day-to-day performance.

5.4 User Classes and Characteristics

5.4.1 Registration Personnel

Registration personnel refers to individuals responsible for creating, retrieving, and managing client files at the health facility. In practice, these activities may be manual (fully paper-based system), semi-automated (combination of both paper and paperless systems), or fully automated (fully paperless system). Where a digital system is available, client files may be managed within one facility-wide HMIS or under multiple specialized applications focused on individual service areas such as EMRs, PIS, LIS, and Radiology Information System (RIS). The role of client registration may be assigned to dedicated personnel or be part of the responsibilities of other officers at the health facility such as nurses or health records officers.

Within the HIS used in the facility or at the individual service points where they are stationed, registration personnel have access to the full set of client demographic information managed under the system. As such, they can search for clients, enroll new clients, and update demographic details for existing clients. In order to adequately meet the needs of this user class, the KPR will cleanly integrate with existing client file management systems to facilitate unique client identification without adversely affecting the regular activities of the registration personnel. Registration personnel will not have access to clients' clinical information.

5.4.2 Health Professionals

Health professionals are health facility staff responsible for delivering healthcare to clients. These include nurses, clinical officers, doctors, nutritionists, laboratory technicians, radiologists, physiotherapists, pharmacists, etc. Typically, health professionals interact with clients once they have been processed by the registration personnel, i.e., once their file has been created or retrieved and the client has been positively identified and placed in the service queue. However, under exceptional circumstances, a health professional may wish to validate a client's identity by querying the KPR e.g., when a client's identity is doubtful or if their demographic details are needed to query another third-party application such as an SHR. Like the registration personnel, health professionals connect to the KPR through their regular HIS terminals. Health professionals generally have unrestricted access to clients' clinical information depending on the roles that they play.

5.4.3. System Administrators

System administrators include all staff responsible for ensuring the smooth running of the CR. They include software engineers, database administrators and network specialists. These professionals use the KPR primarily for troubleshooting, quality assurance (e.g., merging duplicates) and general system administration. Unlike registration personnel and health professionals, system administrators are not based at the health facility but rather at a central location. As such, they access the KPR through a dedicated web interface that allows them to perform their system administration functions. System administrators have full access to the data on the KPR subject to the applicable levels of authentication and audit trailing. However, they do not have access to clients' clinical information. They also have authority to assign roles in the system as required.

5.4.2 Help Desk Personnel

Help desk personnel are individuals responsible for fielding, curating, documenting, and reporting back on technical support queries related to the KPR (e.g., system malfunctions or outages). Help desk personnel may address such queries themselves or pass them on to the more knowledgeable system administrators for investigation and resolution. Like system administrators, help desk personnel are not based at the health facility but rather in a central location. As such, they access the KPR through a dedicated web interface that allows them to perform their technical support functions. Help desk personnel have full access to the data on the KPR subject to the appropriate authentication protocols and audit trailing. However, they do not have access to clients' clinical information.

5.5 Operating Environment

The KPR will be centrally hosted at the national health data center. It will be accessed by system administrators and help desk personnel via a secure web application interface. Client applications such as EMRs will access the KPR via the general-purpose DHP interoperability platform and a well-defined Representational State Transfer (REST) API. Fingerprint readers or any other necessary biometric devices will be provided at all applicable points of service to facilitate the collection and querying of client biometric data. For the purposes of redundancy, reliability, and efficiency, health facilities may keep a local copy of the data obtained from the KPR in order to speed up future searches and ensure that these work with or without outbound connectivity.

5.6 Assumptions

This SRS is based on the following substantive assumptions:

- Participating health facilities will be equipped with the necessary software, infrastructure, and network connectivity to perform their client information management digitally and interoperate with other HIS solutions, including the CR.
- Both existing and future client-facing applications that are deployed at the point of service will be equipped with a special interface to the KPR (“KPR Interface”) to support querying, enrollment, updating, merging, and archiving of data in the registry.
- A robust interoperability platform will be deployed to orchestrate information exchange between various HIS including between the KPR and client applications. The platform will be responsible for message routing and transport layer security.
- Users of HIS at the health facility level will be adequately trained in the use of the KPR to resolve client identities, enroll new clients, update existing clients, detect, and verify duplicates and archive deceased individuals.

SECTION 6: EXTERNAL INTERFACE REQUIREMENTS

6.1 User Interfaces

The KPR will offer a secure web interface that will be used by system administrators and help desk personnel to access the system. Registration personnel and health professionals will access the KPR via custom user interface (UI) modules embedded within their regular HIS (e.g., HMIS, EMRs, PIS). In both cases, the user interface will be designed to be clear, simple, consistent, direct and user- driven. Special attention should be paid to ensuring that users are provided with informative feedback upon taking actions on the user interface, as well as opportunities to reverse those actions when errors occur. The user interfaces embedded within HIS will be designed to correspond to the design language of the native application while at the same time fulfilling the KPR functionality described in the system features section (section 7).

6.2 Hardware Interfaces

The KPR will be built to run on a 64-bit Linux server with at least 32 GB of Random Access Memory (RAM), Core i7 Intel Processor (or equivalent) and a 1TB Solid State Drive (SSD). These are the minimum requirements to enable testing in a relatively cost-effective environment. The production server will have superior specifications. The hardware at the terminals accessing the KPR will be implementation specific and will include suitable laptops, smartphones, and tablets, as necessary. Fingerprint sensors (or any other suitable biometric devices) for collecting biometric data during querying, enrollment, and updating of client demographic data will also be required.

6.3 Software Interfaces

The KPR will provide a well-formed REST API through which external applications will communicate with the system according to the functionality and workflows documented in the system features section (section 7). As part of the KPR distribution, plugins, and reference implementations for embedding user interfaces for the KPR within various HIS will also be provided. Messages between the KPR and third-party applications will be implemented to conform to common patient demographic data management standards such as PIX/PDQ or similar. The DHP interoperability platform will interface with the KPR through the KPR REST API and will be responsible for message routing between nodes as well as TLS.

6.4 Communications Interfaces

Communication between the KPR and third-party client applications will be through a 256-bit encrypted HTTPS connection facilitated via the DHP interoperability platform. The interoperability platform will also be responsible for message routing between nodes to ensure that applications can be migrated to new physical addresses on the network without compromising message transmission.

SECTION 7:
SYSTEM FEATURES

As a centrally hosted system that provides identity resolution services globally, the KPR is accessible to other applications through a general-purpose interoperability platform. The interoperability platform is responsible for facilitating communication between various HIS - including other centrally hosted systems like the shared health record (SHR), district health information system (DHIS), and Kenya master health facility List (KMHFL). End users (registration personnel and health professionals) will connect to the KPR through the applications they already use at their point of service. These include HMIS, EMRs, PIS, LIS, RIS, etc. On the other hand, KPR system administrators and help desk staff access the system directly through a specialized web interface. Figure 1 is an overall depiction of the KPR showing how it relates to other HIS.

The KPR comprises a database that stores client identity data, a business logic layer that facilitates interaction with the database, an API that acts as a gateway to the system's functionality and a web interface that provides the means for system administrators and help desk personnel to interact with the CR. End users (registration personnel and health professionals) interact with the system using the information systems available at their terminals (e.g., HMIS, EMRs, and PIS as depicted above). These applications connect to the KPR via the KPR API, facilitated by the DHP interoperability platform. The sections below describe the key features provided by the KPR in detail.

7.1 Querying for Client Identity

7.1.1 Description

Querying refers to the process of searching for a client's demographic information from the KPR based on known attributes about the client. The demographic information so retrieved constitutes the client's identity data and is used to disambiguate between two or more clients for the purpose of unique identification. More importantly, each client's demographic data is indexed by a UUID that is used to distinctly identify the client's records across the health system. The UUID is assigned at the point of enrolling the client into the CR. The client demographic information managed under the KPR is selected to maximize the chances of correct identification. It also takes into consideration additional factors such as acceptability, convenience, confidentiality, query performance and compliance with relevant legislation. The full set of client demographic information managed under the KPR is documented in the Enrollment section.

7.1.2 Stimulus/Response Sequence

To initiate a client search, the user submits to the KPR one or more query parameters based on the known attributes of the client. Query parameters are any combination of variables that comprise the client's demographic information managed within the KPR (e.g., National ID number, first name, last name, fingerprint data). The specific query parameters sent to the KPR are determined by the user based on the information available to them at the point of service. For example, a query for a disoriented or unconscious client might include only biometric and sex data, while one for a fully conscious client might include their National ID number, names, and other variables that help narrow down the search and increase the chances of a correct, unambiguous, and efficient match.

Once the KPR receives a query, it services it by performing a deterministic, probabilistic, or biometric search depending on the query parameters submitted. For example, if the National ID is included as a query parameter, then a deterministic search is performed. If the first and last names are included in the query, a probabilistic search is performed. If fingerprint data is also included, a biometric search is executed. Whatever algorithm or combination of algorithms are used, the KPR returns one of the following responses upon completing the search:

- **No Match**: If no match is found for the submitted query, the KPR returns a response indicating that no match was found.
- **Matches**: If one or more matches are found for the submitted query, the KPR returns a response containing a list of those matches.

Each match returned contains the full set of demographic information available for the client. It also contains a UUID that distinctly identifies the client across the health system. The UUID forms the basis for identifying that client's health records in all transactions generated at any point of health service provision regardless of physical location. Figure 6 depicts an overview of the querying process.

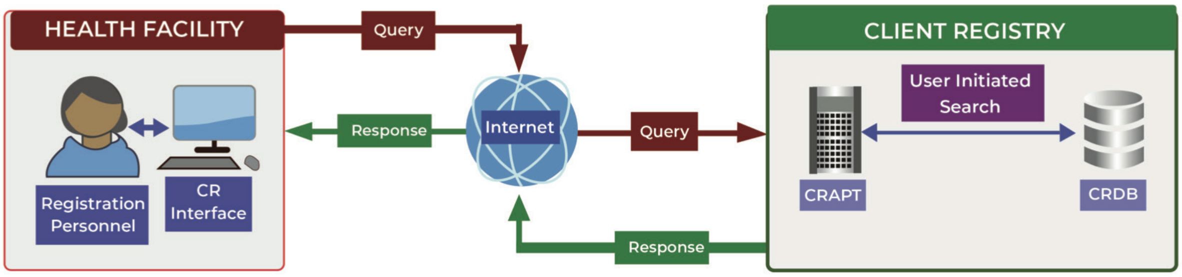

Figure 6 - An overview of the KPR querying process

Query Example 1

The registration personnel will collect one query parameter (National ID) from the client and submit it to the KPR through the KPR interface. The KPR interface forwards the query via the KPR API. The KPR performs a deterministic search in its database and finds that the query parameters match exactly one client. The match is returned to the KPR interface in a response message containing the client's full demographic details.

Query 1	Response
National ID: 123456789	<u>**Match 1 (Score: 100%)**</u> **UUID:** 7df89584-532f-11eb-a742-131259fd843d **National ID:** 123456789 **Sex:** Male **First Name:** James **Middle Name:** Omolo **Last Name:** Ouma **DOB:** May 1, 1980 ... Etc. (Additional client details)

Query Example 2

The registration personnel will collect three query parameters (sex, first name, and last name) from the client and submits them to the KPR through the KPR interface. The KPR interface forwards the query through the KPR API. The KPR performs a probabilistic search in its database and finds that the query parameters match three clients. The matches are returned to the KPR interface in a response message containing each of the three clients' full demographic details. Note that the CR's probabilistic algorithm accommodates minor variations of client details such as spelling errors.

Query 2	Response
Sex: Male **First Name:** James **Last Name:** Ouma	**Match 1 (Score: 100%)** **UUID:** 7df89584-532f-11eb-a742-131259fd843d **National ID:** 123456789 **Sex:** Male **First Name:** James **Middle Name:** Omolo **Last Name:** Ouma **DOB:** May 1, 1980 ... Etc. (Additional client details)
	Match 2 (Score: 100%) **UUID:** ae45a98e-532f-11eb-a174-a750eb8c1fd **National ID:** 234567891 **Sex:** Male **First Name:** James **Middle Name:** Oloo **Last Name:** Ouma **DOB:** December 28, 1989 ... Etc. (Additional client details)

Query Example 3

The registration personnel collect two query parameters (sex and fingerprint) from the client and submits them to the KPR through the KPR interface. The KPR interface forwards the query through the KPR API. The KPR performs a biometric search in its database and finds that the query parameters do not match any client. It sends back a response indicating that no matches were found.

Query 3	Response
Sex: Male **Fingerprint (Binary Data):** VGhpcyBiYXNlIDY0IGVuY29kZWQgZGF 0YSByZXByZXNlbnRzIGEgcGxhY2Vob2 xkZXIgZmluZ2VycHJpbnQgaW1hZ2UgZ m9yIHVzZSBpbiB0aGUgY2xpZW50IHJl Z2lzdHJ5IGRvY3VtZW50Lg==	**No matches found**

7.1.3 Workflow

The flowchart in figure 7 depicts the workflow for using the KPR to uniquely identify clients at the point of service.

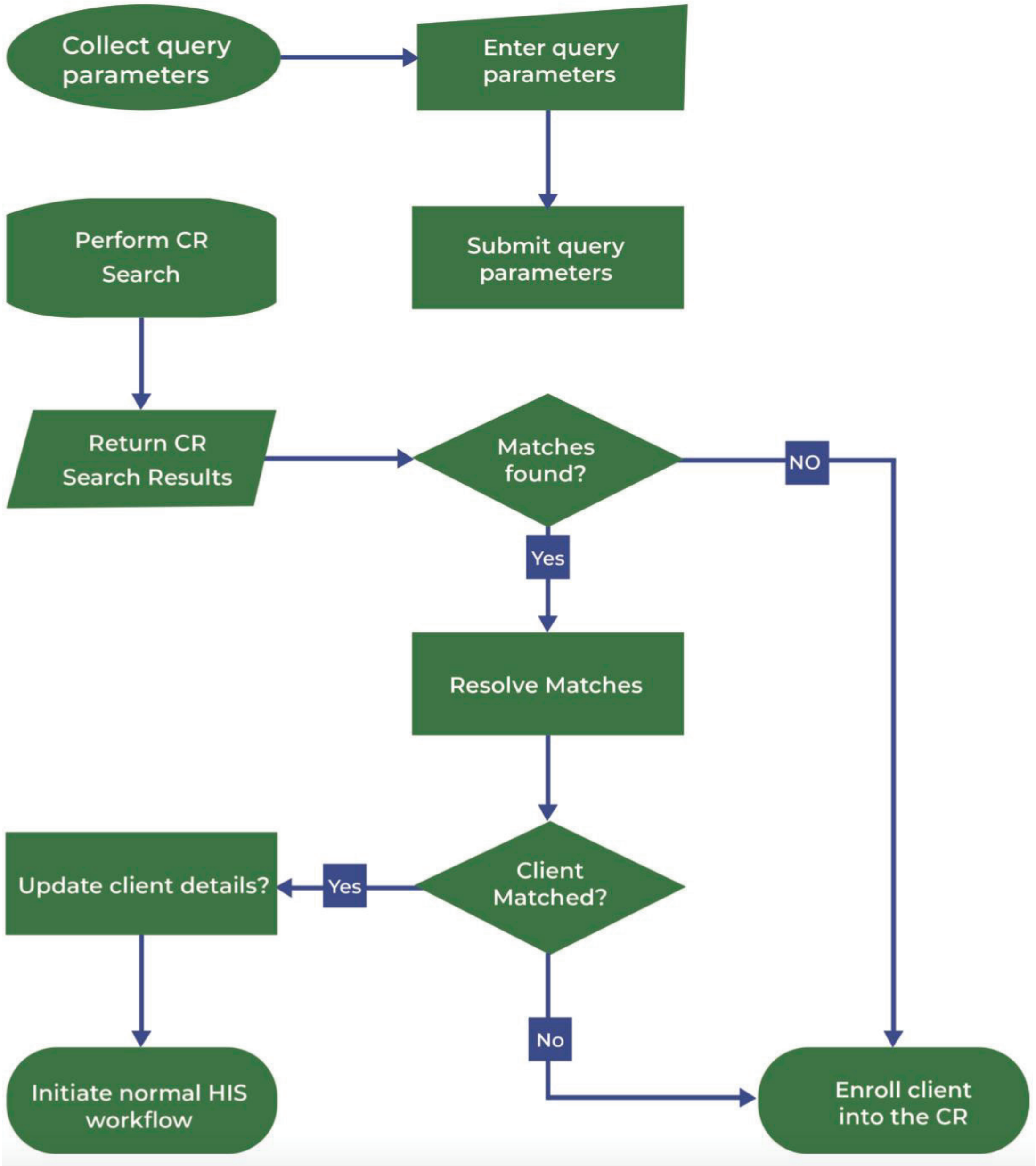

Figure 7 - Client identification workflow

- **Collect query parameters:** The user collects known attributes from the client which he wishes to submit as query parameters
- **Enter query parameters**: The user enters the query parameters into the KPR interface for submission to the CR
- **Submit query parameters:** The KPR interface forwards the query parameters to the KPR through the KPR API
- **Perform KPR search:** The KPR performs a deterministic, probabilistic, and/or biometric

search for the client based on the query parameters

- **Return KPR results:** The KPR returns the results of the search, i.e., either no matches found, or a list of the matches that were found
- **Matches found:** If some client matches are returned by the CR, the user resolves the matches, otherwise he proceeds to the client enrollment workflow
- **Resolve matches:** The user checks if any of the matches received correspond to the client in front of them, i.e., by comparing additional attributes not included in the query
- **Client matched:** If a match for the client is found, the user optionally updates their details and then initiates the normal HIS workflow. Otherwise, he enrolls the client
- **Update client details:** The user may update a client's demographic details if these have changed, or additional information has become available
- **Initiate normal HIS workflow:** Start the usual workflow for processing the client within the KPR interface e.g., placing the client in the clinician's queue in the EMR
- **Enroll client into CR:** Enroll the client into the KPR to facilitate unique identification in future

7.1.4 Additional Notes

The KPR should support deterministic, probabilistic, and biometric search algorithms. The specific algorithm(s) to be used should be selected dynamically based on the query attributes submitted.

The KPR should allow for search algorithms to be configured for optimal performance. For example, the KPR system administrator should be able to choose between various edit distance algorithms as well as set probabilistic matching thresholds.

Client matches in the response message from the KPR should be ranked based on the degree to which they match the query parameters. The closest match should be ranked at the top while the farthest match should be ranked at the bottom.

Query messages from the KPR interface to the KPR should not be queued, as responses received in the absence of the client are not useful. In the absence of connectivity to the CR, a temporary client enrollment may be conducted and marked for later resolution.

Previous query results may be locally cached to speed up future searches. In this case, the KPR interface is responsible for caching and for searching in the local cache before or in conjunction with a remote search at the centralized CR.

7.2 Enrolling New Clients

7.2.1 Description

Enrollment refers to the process of adding a new client's demographic information into the CR. In order to reduce the chances of the same client being enrolled more than once, every enrollment should be preceded by a client search. This means that operationally, the user should perform a search before enrollment. However, because a proper user-initiated search cannot be guaranteed, an automated client search should also be performed before any enrollment request is processed. If any matches are found because of the automated pre-enrollment search, the enrollment request should be suspended, and the user offered an opportunity to confirm whether any of the matches correspond to the client for whom the enrollment request was raised.

Table 5 shows the full set of demographic information that may be submitted during enrollment. The variables have been selected to maximize the chances of correct client identification while taking into consideration additional factors such as acceptability, convenience, confidentiality, performance, and compliance with relevant legislation. These attributes constitute all the client data managed under the KPR for the purposes of unique identification. Certain attributes require that the indicated official proof of ownership be provided before they can be entered into the CR.

Table 5 - Demographic information that may be submitted during enrollment

Attribute	Mandatory	Proof Required
UUID	Yes	None
Huduma Namba	No	Huduma Card
National ID Number	No	National ID
Passport Number	No	Passport
Telephone Number	No	None
First Name	Yes	Huduma Card/National ID/Passport/Birth Certificate/Driving License/Student ID
Middle Name	No	Huduma Card/National ID/Passport/Birth Certificate/Driving License/Student ID
Last Name	Yes	Huduma Card/National ID/Passport/Birth Certificate/Driving License/Student ID
Mother’s Maiden Name	Yes	None
Fingerprint 1	No	Finger 1
Fingerprint 2	No	Finger 2
Sex	Yes	None
Date of Birth	Yes	None
Place of Birth	Yes	None
Place of Registration	Yes	Automatic
Alive	No	Death Certificate

7.2.1 Stimulus/Response Sequence

Operationally, enrollment is performed when a thorough client search results in no matches. This indicates that the client’s demographic information does not exist on KPR and as such needs to be added to facilitate unique identification in the future. To initiate an enrollment, the user submits all the available client demographic information to the CR. Where official proof is required but not provided, registration may proceed without the affected attributes. First name, middle name, and last name are exempted from this rule and may be entered into the KPR without proof to facilitate temporary identification awaiting validation (figure 8).

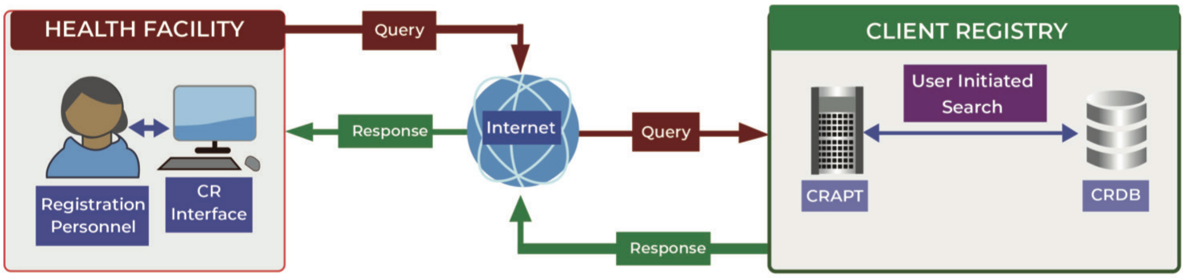

Figure 8 - KPR enrollment overview

Upon receipt of the enrollment request, KPR automatically conducts a search in the same way it would if the request were a search query. This serves the purpose of arresting any potential duplicates before they arise. If one or more matches are found during this search, the KPR temporarily interrupts the enrollment and returns a search response instead. This offers the user an opportunity to verify whether the demographic details submitted for enrollment into the KPR represent a new client. If the user indicates that the client is new, the KPR completes the enrollment by saving the client's demographic details. The KPR interface is responsible for generating the client's UUID. This ensures that client enrollments can be processed locally in the absence of a connection to KPR (*see more details in the Additional Requirements section*).

7.2.2 Workflow

The flowchart in figure 9 depicts the workflow for enrolling a new client into the CR. Operationally, this workflow is initiated after a client search yields no positive matches (see querying workflow on figure 7).

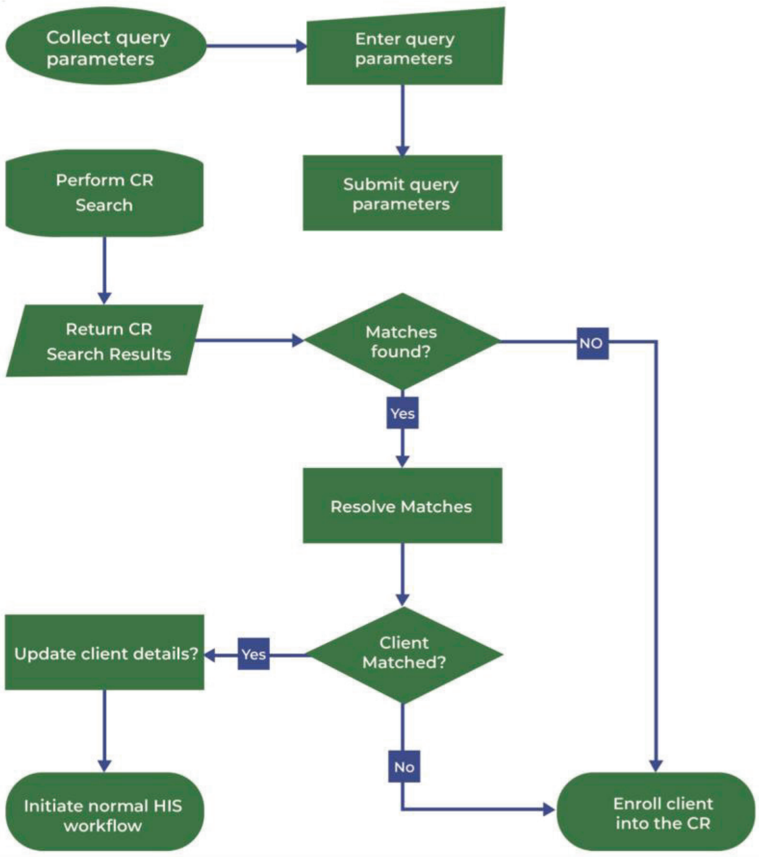

Figure 9 - Client enrollment workflow

- **Collect client attributes:** The user collects all available client attributes that comprise the client's identity data in the CR
- **Enter client attributes:** The user enters the available client attributes into the KPR interface for submission to the CR
- **Submit client attributes:** The KPR interface forwards the client attributes to the KPR through the KPR API
- **Perform automatic KPR search:** The KPR automatically performs a deterministic, probabilistic and/or biometric search for the client based on the query parameters.
- **Matches found:** If some possible client matches are found by the CR, the enrollment process is suspended, and the matches are returned to the user
- **Suspend client enrollment:** Suspending client enrollment when KPR finds potential matches reduces the chances of the same client being enrolled more than once
- **Return KPR results**: The KPR returns the results of the automated search with the list of all potential matches found
- **Resolve matches:** The user checks if any of the matches received correspond to the client in front of them, i.e., by comparing additional attributes not included in the query
- **Client matched:** If a match for the client is found, the user optionally updates the client's details and then initiates the normal HIS workflow. No enrollment is performed

- **Update client details:** The user may update a client's demographic details if they have changed, or additional information has become available
- **Initiate normal HIS workflow:** Start the usual workflow for processing the client within the KPR interface (e.g., placing the client in the clinician's queue in the EMR).
- **Restart client enrollment:** If no client match is found from the automatic search, the suspended client enrollment process is restarted
- **Enter client attributes into the CR:** The client's attributes are entered into the KPR to facilitate unique identification in future and the normal HIS workflow is initiated

7.3 Updating Existing Clients

7.3.1 Description

Updating refers to the process of modifying demographic information belonging to clients whose information already exists in the CR. Maintaining the most up-to-date data on clients within the KPR is important for facilitating unique client identification. Client data may be updated to include additional information, correct errors, or reflect legitimate changes in personal data such as a name change arising from marriage. For a client's record to be updated on the CR, their details must first be retrieved through the querying process described earlier. An update request containing the updated information is then submitted to the KPR against that client's UUID. Since all systems track client data based on the UUID, an update to client data does not need to be cascaded beyond the CR. Any of the client attributes managed under the CR, except "alive," may be updated under this workflow manner. The alive attribute is updated as described in the archiving process.

7.3.2 Stimulus/Response Sequence

Updating is performed upon a successful KPR search that yields a positive client match. Updating is optional and is only initiated if the client's details need to be modified, i.e., to include additional attributes or update existing ones. To initiate an update, the user submits the updated client demographic information to the CR. Where official proof is required but not provided, updating may proceed without the affected attributes. First name, middle name and last name are exempted from this rule and may be updated in the KPR without proof and validated later. Upon receipt of the update request, KPR updates the database immediately, using the UUID retrieved through the querying process to index the updated record.

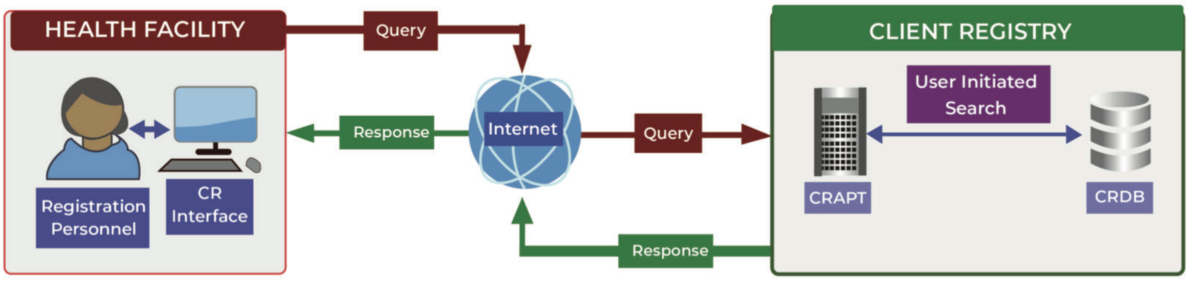

Figure 10 - Overview of client data update

7.3.3 Workflow

The flowchart figure 10 depicts the workflow for updating an existing client's details in the CR. This workflow is initiated (optionally) after a client search yields a positive match (see querying workflow on figure 7).

- **Collect updated client attributes**: The user collects the client's attributes that need to be updated, i.e., new or modified information
- **Enter updated client attributes**: The user enters the updated client attributes into the KPR interface for submission to the CR
- **Submit updated client attributes**: The KPR interface forwards the updated client attributes to the KPR through the KPR API
- **Save updated client attributes**: The KPR saves the updated client attributes into the KPR indexed by the UUID
- **Initiate normal HIS workflow**: The usual workflow for processing the client within the KPR interface is started (e.g. placing the client in the clinician's queue in the EMR).

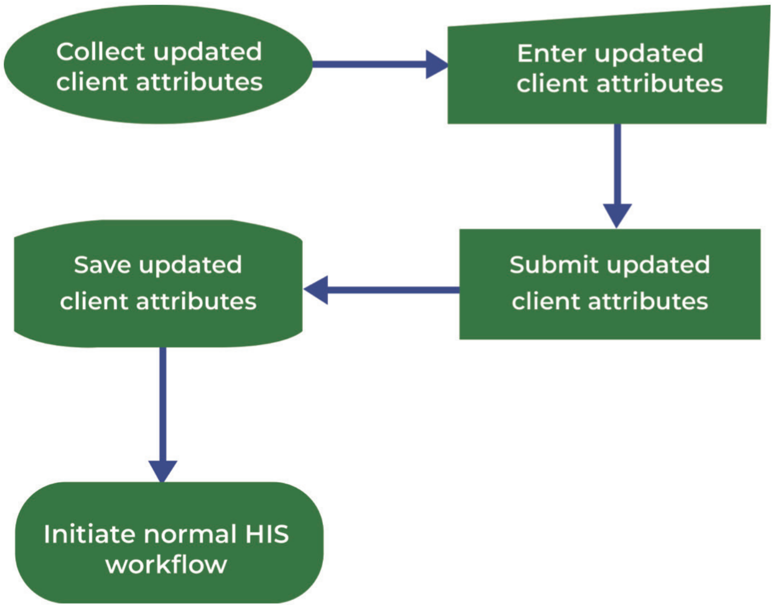
Collect updated client attributes
Enter updated client attributes
Submit updated client attributes
Save updated client attributes
Initiate normal HIS workflow

Figure 11 - Client update workflow

7.4 Merging Duplicates

7.4.1 Description

Merging refers to the process of combining two or more client records in the KPR that are determined to belong to the same client but are entered as different clients, each with a different UUID. The result of a merger should be one client record in the KPR indexed by one UUID. Merging is a critical operation because it has potentially dangerous implications on individual care and/or on data quality for public health programming. For example, merging two clients erroneously can assign one client's allergies to the other, thereby limiting the non-allergic client's access to potentially lifesaving medication. Similarly, erroneously merging clients who are separate individuals can lead to underreporting in service statistics. For this reason, caution must be taken before merging client records in the CR.

Generally, the following three possibilities could lead to duplicate client records in the CR.

- **Intentional misrepresentation:** A client intentionally misrepresents their identity during enrollment and as a result is enrolled under multiple identities. This possibility can be mitigated by requiring official proof of identity during enrollment
- **Poor querying technique:** Registration personnel fail to conduct a thorough client search and identity resolution before enrollment. This possibility can be mitigated by proper user training and through the automated pre-enrollment search
- **Technical hitches:** Registration personnel fail to connect to the KPR due to technical challenges and therefore perform a provisional enrollment locally. This possibility can be mitigated through enhanced KPR availability and prompt technical support.

Once a duplicate occurs in the CR, it must be detected, verified, and resolved. Duplicate detection refers to the process of noticing or flagging suspected duplicates. Duplicate verification, on the other hand, refers to the process of checking whether a detected duplicate represents an erroneous multiple entry for the same client or is simply a false positive. Lastly, duplicate resolution refers to the process of merging verified duplicates to create a single client identity in the CR. Duplicates may be detected manually at the point of service during a routine KPR query or automatically by an algorithm that runs periodic duplicate checks on the CR. The process for detecting duplicates involves an equivalence analysis between two or more client identity records with the goal of generating a similarity score. Records with a high enough similarity score are flagged as possible duplicates awaiting verification and resolution.

7.4.2 Stimulus/Response Sequence

The responsibility of verifying duplicate client records identified in the KPR belongs to the registration personnel. Suspected duplicates may come to their attention in one of the following 2 ways.

- **During routine KPR queries:** Registration personnel perform a search and notice two or more matches that appear equivalent (e.g., two clients with the same National ID number and/or fingerprint data).
- **Notifications generated automatically by the CR**: Background duplicate flagging algorithm detects two or more client matches that appear equivalent (e.g., two clients with the same National ID number and/or fingerprint data).

In either case, the registration personnel undertake a duplicate verification process. This process occurs outside the system and may involve asking the client additional questions or liaising with healthcare delivery professionals to review a client's medical records. The specific standard operating procedure (SOP) for this process is outside the scope of this specification. The result of the verification process is a determination as to whether the two or more records suspected to be duplicates are indeed duplicates or simply false positives. Upon positive verification, registration personnel raise a merger request through the CR. The request is presented to the system administrator, who executes the merger in the database if satisfied with the assessment of the registration personnel. Otherwise, the system administrator may conduct additional investigation to verify the duplicate. This completes the merging process.

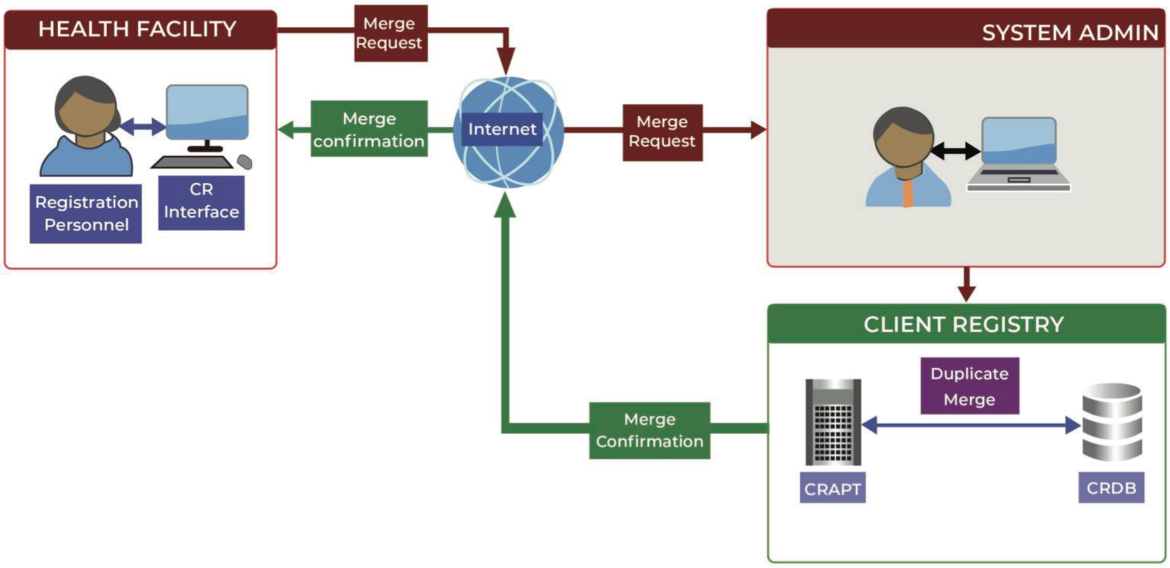

Figure 12 - Overview of the duplicate merging process

7.4.3 Workflow

The flowchart below depicts the workflow for identifying suspected duplicates, verifying them, and resolving them in the CR.

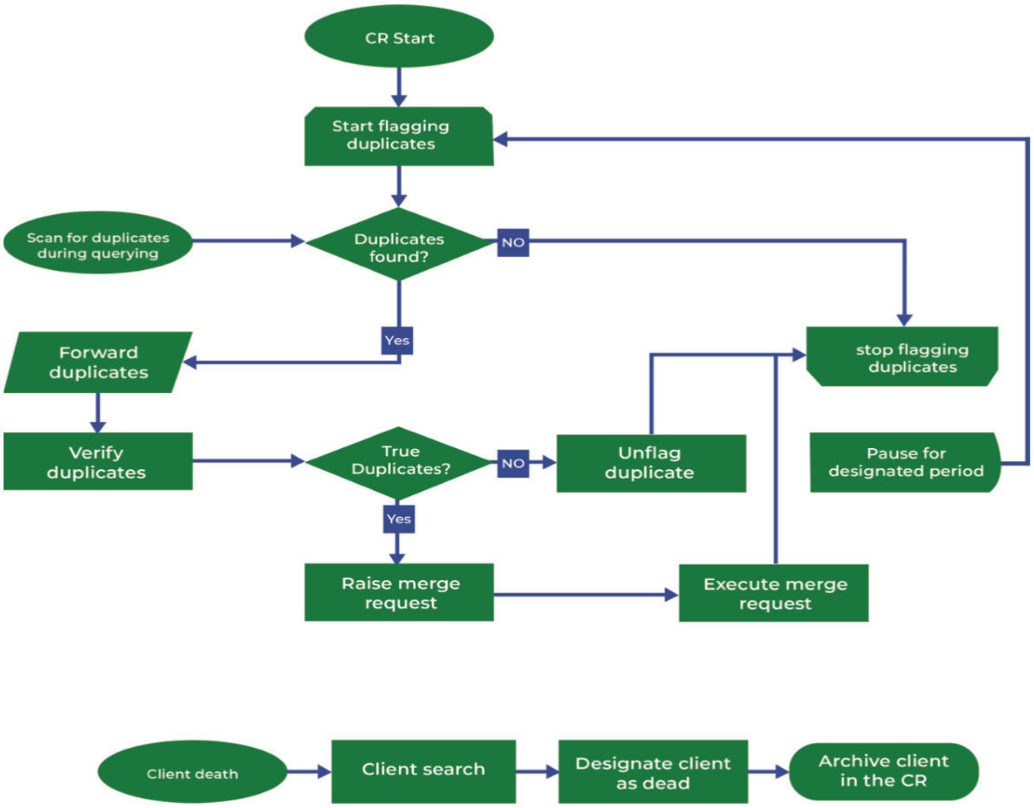

Figure 13 - Merging workflow for resolving duplicates

- **KPR Start:** The KPR is started, either for the first time or as a restart following a scheduled or unscheduled shutdown.
- **Start Flagging Duplicates:** The background KPR algorithm for flagging duplicates is started. It compares clients in the database for similarities that indicate potential duplication.
- **Scan for Duplicates During Querying:** During routine KPR querying, registration personnel scan the results to identify suspected duplicates.
- **Duplicates Found:** If any clients appear to be duplicates, they are forwarded to the health facility for resolution, otherwise the flagging algorithm pauses.
- **Forward Duplicates:** The KPR forwards suspected duplicates to the respective facilities where they originated. This only happens if duplicates are detected algorithmically.
- **Verify Duplicates:** Upon receiving the suspected duplicates, the registration personnel at the facility checks whether each duplicate is indeed true or false.
- **True Duplicate:** If a duplicate is positively validated, then it is resolved on the CR. Otherwise, the duplicate is unflagged on the CR.
- **Raise Merger Request:** If a duplicate is positively verified, registration personnel raise a merger request to the KPR system administrator.
- **Execute Merge Request**: If the system administrator is satisfied that two records are indeed duplicates, they merge them in the CR.
- **Unflag Duplicate:** If a suspected duplicate is identified as a false positive, it is unflagged in the KPR and the system knows to not flag that duplicate in future.
- **Stop Flagging Duplicates:** The duplicate flagging algorithm is configured to stop periodically to save system resources.
- **Pause for Designated Period:** During this step, the KPR duplicate flagging process is paused for a specified period to save system resources.

7.5 Archiving Dead Clients

7.5.1 Description

Archiving refers to the process of physically or logically migrating an existing client's identity data on the KPR to a less frequently accessed part of the system. The goal of archiving is to promote system performance by ensuring that less frequently accessed data does not slow down queries, enrollment, updating, duplicate detection, merging, or any other KPR operations. However, archived client data can still be queried subject to an explicit request to that effect embedded in the query. Operationally, clients are archived in the system when they die, as this indicates the end of their consumption of healthcare services. Possible reasons for querying archived client data may include servicing lawful information requests such as court orders, medical review, and/or research purposes.

7.5.2 Stimulus/Response Sequence

Client record archiving is initiated by the confirmation of the death of the client. Upon this confirmation, registration personnel are notified to initiate the archiving process in the CR. Ideally, this notification should be automated within the HIS (e.g., EMR). However, it can also be raised manually by simply notifying the registration personnel of a client's death. Upon notification, the registration personnel will perform a client search in the KPR to retrieve the client's record. He then uses the KPR interface to designate the client as dead, which in turn results in a client archival request to the CR. The KPR processes the request by migrating the client's identity data to the archive.

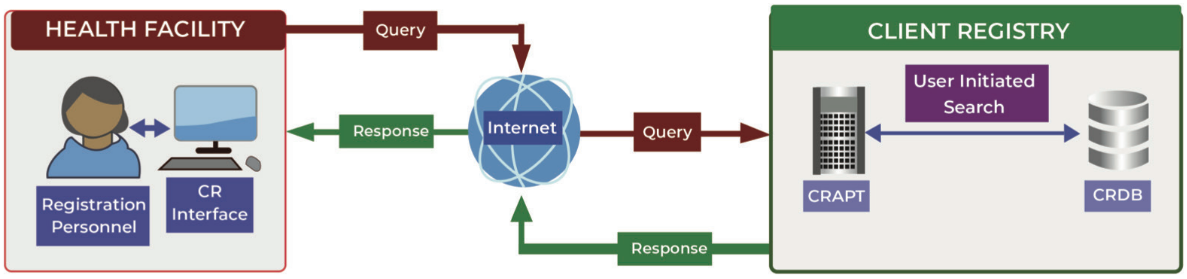

Figure 14 - Client archiving overview

7.5.3 Workflow

The flowchart above (figure 14) depicts the workflow for archiving clients in the CR.

- **Client Death:** A client death occurs and is lawfully certified by an authorized health practitioner.
- **Client Search:** Registration personnel are notified of the death and perform a search to retrieve the client's record from the CR.
- **Designate Client as Dead:** Through the KPR interface, the registration personnel designate the client as dead and submit this information to the CR.
- **Archive Client in CR:** The KPR receives the information that the designated client is dead and subsequently archives the client's identity data.

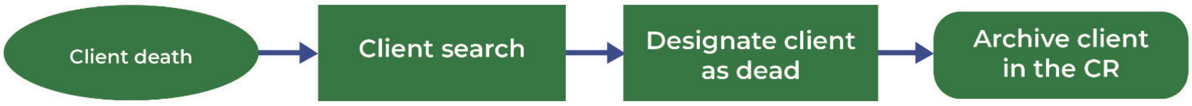

Figure 15 - Client archiving workflow

SECTION 8:
NON-FUNCTIONAL REQUIREMENTS

8.1 Data Security

Data security refers to the assurance that the data transmitted to and from a system as well as the data stored within it has the necessary security measures in place to deter unauthorized access. Clinical data and identity are inherently confidential and therefore, the KPR system must adhere to the most stringent industry-standard information security practices. The KPR will be designed to comply with the latest information security standards in order to ensure that the sensitive client data processed through it is adequately secured. In particular, the KPR shall implement a robust mechanism for user authentication backed by strong hashed and salted passwords for individual user accounts, PKI to limit administrator access to data servers to authorized devices only, 256-bit TLS encryption to encrypt data in transit and prevent eavesdropping attacks, role based access control, inactivity timeouts and audit trailing; software and hardware firewalls; intrusion monitoring; regular software updates; and staff training and sensitization on data security and confidentiality best practices.

8.2 Data Integrity

Data integrity focuses on the validity, consistency and accuracy of data that is stored within a system. The KPR implementation team will review and identify all common threats that would compromise data quality and define the necessary mitigation measures to be implemented in the system. Examples of such threats include human error, hardware failure, misconfiguration, security errors, data transfer errors, and cyberattacks. Possible mitigation measures include input validation, routine deduplication, data audit trailing, data backup, and access control.

8.3 Usability

Usability is the ease in which the users can interact with a system while having their goals effectively fulfilled. The KPR implementation team shall promote optimal usability of the system by implementing easy-to-use and intuitive user interfaces that blend into the users' daily workflow, showing helpful error messages (with recovery instructions where applicable); specifying meaningful defaults for common data entry fields; minimizing or eliminating distracting and non-essential features; developing and running usability tests on prototypes with an appropriate audience before scale up; referencing successful applications for best practices; customizing the system to reflect the users local language, culture, and/or literacy level; and other similar considerations.

8.4 Performance and Scalability

Performance is an indication of the responsiveness of a system to execute any action within a given time interval. Scalability refers to the ability of a system either to manage increases in load without impact on performance or for the available resources to be readily increased. Appropriate provisions must be made to scale the KPR service capacity in terms of both hardware resources and application-level optimizations. The KPR will be designed for optimal performance and scalability by defining specific metrics for system throughput and latency.

Automated tests will be used to simulate a large number of requests to stress-test the system and identify and fix bottlenecks.

8.5 Reliability

Reliability refers to the ability of a system to run without experiencing a failure for any given period under a set of predefined conditions. The KPR shall ensure reliability by supporting database replication for redundancy, load balancing, and routine monitoring of system logs to identify and resolve technical errors and performance bottlenecks before they manifest themselves to system users.

8.6 Maintainability

Maintainability refers to the amount of time taken for system maintenance, upgrade, or performance optimization. It defines the ease and speed with which a system can be restored to operational status after a failure occurs or a modification is requested. As such, maintainability is a major enabler of reliability, as it has a direct impact on system uptime and performance. The specific proposed strategies for promoting the maintainability of the KPR system include clear and concise code, separation of concerns, modularization, unit testing, continuous integration, technical documentation, and general conformance to software design and development best practices.

8.7 Availability

Availability is the likelihood that a given system will be available to users at any given time. The KPR shall promote the achievement of availability by implementing redundancy measures to decrease the likelihood that the system is not available to users on demand.

8.8 Interoperability

Interoperability refers to the ability of computer systems or software to exchange and make use of information. Interoperable health information systems should be able to exchange, interpret, and use data in a cohesive and consistent way. The KPR is expected to exchange data with other systems including the NIIMS, EHR systems, the KHIS, the SHR, among others. In order to fulfill this requirement, the KPR shall adhere to the stipulations documented in the KHIS Interoperability Standards and Guidelines and provide secure APIs for information exchange as appropriate. The KPR will be designed to support all three levels of interoperability namely, foundational, structural, and semantic interoperability. Moreover, participating applications will be required to support RESTful web services and to package their payloads in standard HIE formats, principally HL7 and FHIR.

8.9 Auditability

Auditability refers to the ability of a system to maintain a chronological record of all critical events and procedures occurring within the system to serve as documentary evidence of the sequence of activities affecting the system at any given time. Auditability within the KPR will help system administrators to monitor the system for security breaches and compliance with laid down standard operating procedures.

LIST OF CONTRIBUTORS

	Name	Organization
1.	Agnes Wairimu	MOH
2.	Albert Kinyanjui	MOH
3.	Ali Hassan	MOH-DHI
4.	Allan Barasa	MOH
5.	Amos Mutuku	MOI Huduma Secretariat
6.	Andrew Wamari	MOH
7.	Annastacia Muange	MOH
8.	Beatrice Oyoo	MOH
9.	Brenda Opanga	NASCOP
10.	Charles Atelu	I-TECH Kenya
11.	Cyril Kea	MOH
12.	Dalmas Ayieko	MOH
13.	Daniel Mukhwana	MOH
14.	David Kareko	MOH
15.	Diana Kamar	MOH-DHI
16.	Dorcas Nguyo	MOH-DHI
17.	Dr. Anne Njoroge	I-TECH Kenya
18.	Dr. Ayub Manya	MOH
19.	Dr. David Soti	MOH
20.	Dr. Davies Kimanga	CDC Kenya
21.	Dr. Joseph Sitienei	MoH
22.	Dr. Joyce Wamicwe	MOH
23.	Dr. Martha Muthami	MOH

24.	Dr. Mike Ekisa	DOH-Kakamega County
25.	Dr. Salome Okutoyi	USAID
26.	Dr. Sarah Amadi	MOH
27.	Dr. Violet Oramisi	NASCOP
28.	Dr. Wesley Ooga	MOH-DHI
29.	Erastus Karani	MOH
30.	Eric Maira	MOH
31.	Eric Nderitu	MOH-DHI
32.	Faith Marete	DOH-Nakuru
33.	Faith Ngare	NASCOP
34.	Francis Nyamari	MOH
35.	Francis Nyamari	MOH
36.	George Onyango	NACC HQ
37.	George Owiso	I-TECH Kenya
38.	Gilbert Mboro	MOH-DHI
39.	Gitahi Nganga	Hoji LTD
40.	Gonza Omoro	US DoD

REFERENCES

i. Open Society Justice Initiative, 2019, Kenya's National Integrated Identity Management System (https://www.justiceinitiative.org/uploads/8f3b665c-93b9-4118-ad68- 25ef390170c3/briefing-kenya-nims-20190923.pdf)

ii. Healthcare Information and Management Systems Society (HIMSS), 2020, Interoperability in Healthcare (https://www.himss.org/resources/interoperability-healthcare)

iii. Ministry of Health, 2020, Refocusing on Quality of Care and Increasing Demand for Services; Essential Elements in Attaining Universal Health Coverage in Kenya (https:// www.health.go.ke/wp-content/uploads/2019/01/UHC-QI-Policy-Brief.pdf)

iv. https://www.justiceinitiative.org/briefing-kenya-nims-20190923.pdf

v. http://guidelines.health.go.ke/#/

vi. http://guidelines.health.go.ke/#/

vii. Government of Kenya, 2017, The Health Act (http://kenyalaw.org/kl/fileadmin/pdf-downloads/Acts/HealthActNo.21of2017.pdf)

viii. Government of Kenya, 2019, The Data Protection Act (http://kenyalaw.org/kl/filead-min/pdfdownloads/Acts/2019/TheDataProtectionAct No24of2019.pdf)

ix. http://guidelines.health.go.ke/#/

x. http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionActNo24of2019.pdf

xi. http://guidelines.health.go.ke/#/

xii. https://www.iso.org/home.html

xiii. UNAIDS, 2014, Considerations and Guidelines for Countries Adopting National Health Identifiers (https://www.unaids.org/sites/default/files/media_asset/JC2640_national-healthidentifiers_en.pdf)

xiv. Kenya Universal Health Coverage Information Exchange Reference Model. Interoperability platforms also support healthcare domain specific standards such as HL7, MLLP, DICOM and EDI. Fundamentally, Interoperability platforms come with flexible infra- structure to share and process the data with a variety of entities

xv. National Coordinator for Health Information Technology, 2019, What is an Electronic Health Record? (https://www.healthit.gov/faq/what-electronic-health-record-ehr)

xvi. OpenHIE, 2020, Shared Health Record (https://ohie.org/practice-area/shared-health-record/)

xvii. INTEROPERABILITY PLATFORMS offers an integration patterns and components to support interoperability across the enterprise. The INTEROPERABILITY PLAT- FORMS also supports healthcare domain specific standards such as HL7, MLLP, DICOM and EDI. Fundamentally INTEROPERABILITY PLATFORMS solutions come with flexible infrastructure to share and process the data with a variety of entities.

xviii. Alex DelVecchio, 2017, Enterprise Master Patient Index (https://searchhealthit.techtarget.com/definition/master-patient-index-MPI)

xix. National Coordinator for Health Information Technology, 2011, EMR vs EHR, what is the Difference? (https://www.healthit.gov/buzz-blog/electronic-health-and-medi-cal-records/emr-vs-ehr-difference)

xx. National Coordinator for Health Information Technology, 2019, Consolidated CDA Overview (https://www.healthit.gov/topic/standards-technology/consolidated-cda-overview)

xxi. National Coordinator for Health Information Technology, 2019, How APIs in Health Care can Support Access to Health Information: Learning Module (https://www. healthit.gov/topic/patient-access-to-medical-records/learning-module-apis-and- health-data-sharing)

xxii. Daniel Chaput, 2020, FHIR® and Public Health, Current Activities, Plans, and Future Possibilities (https://www.healthit.gov/sites/default/files/page/2020-03/FHI- RandPublicHealth.pdf)

MINISTRY OF HEALTH

Nairobi, Kenya
Government of Kenya

PUBLISHED BY:
MINISTRY OF HEALTH
AFYA HOUSE, CATHEDRAL ROAD
P.O. BOX 30016 NAIROBI 00100
www.health.go.ke

HEALTH SECTOR UNIQUE IDENTIFICATION FRAMEWORK

AUGUST 2022