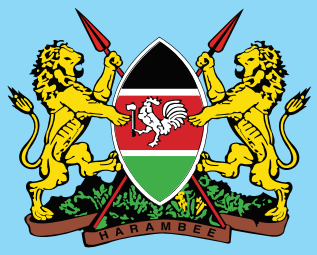
REPUBLIC OF KENYA



MINISTRY OF HEALTH

Kenya Standards and Guidelines for mHealth Systems

April, 2017

FOREWORD

The Ministry of Health recognizes the crucial role that appropriate use of relevant standards and guidelines plays in the implementation of mobile health (mHealth) applications. In this regard, the development of the Kenya mHealth Standards and Guidelines is important as a means of enhancing efficiency and effectiveness in the delivery of health services via mobile platforms in the country. In the public health sector, the Kenya mHealth Standards and Guidelines will ensure that all mHealth based systems and health strategies are correctly applied. The implementation and enforcement of these standards and guidelines will go a long way in reducing duplication of efforts, in promoting data and information sharing among systems, and in harnessing appropriate use of mobile technology as an enabler to effectiveness and efficiency in the delivery of healthcare services.

As the Ministry of Health (MOH) increasingly embraces the use of Information and Communications Technology (ICT) in its service delivery, it is becoming more important to take a common approach based on recognized best practices. The Ministry recognizes the need for a consistent approach to the development of ICT systems and, thus, the need to formulate these standards and guidelines.

The standards and guidelines set out in this document shall apply to the health sector at all levels of healthcare and health management both at the national and county government level to support service delivery and to facilitate referral mechanisms utilizing mobile technologies. This document provides the much-needed guidance towards establishing, acquiring and maintaining current and future mobile based health information systems and ICT infrastructure that foster data and information sharing across multiple systems.

This document was developed through a participatory process involving stakeholders in health, including government ministries, agencies, civil society organizations and development partners. Valuable input was received from various experts in different fields and interests. These national standards consistent with internationally recognized standards and guidelines are to be implemented in accordance with the existing and relevant policies, legal framework, strategies and standards including Health Policy, ICT Standards, System Interoperability Principles and the Health Information Policy.

Lastly, it is my sincere hope that all the stakeholders in the health sector will support these standards and guidelines to ensure that we steer the country towards the use of acceptable standards so as to improve the overall health of our citizens.

Dr. Kioko Jackson K., OGW
Director of Medical Services

ACKNOWLEDGEMENT

The Kenya mHealth Standards and Guidelines were developed, reviewed and finalized through the tremendous efforts and commitment of various individuals and organizations.

We would like to acknowledge the contributions of the Ministry of Health leadership led by Cabinet Secretary Dr. Cleopa Mailu, and the Principal Secretary Dr. Nicholas Muraguri, whose leadership ensured that the document was completed. Special thanks go to the Director of Medical Services Dr. Jackson Kioko; and Dr. Peter Kimuu, the head of the Department of Policy Planning and Health Care Financing whose enormous support and guidance ensured that there was full participation of ministry staff and stakeholders in the entire process. Also critical from the inception to the final stages were the personal support and contributions of the former Head of Division Monitoring & Evaluation, Research Development and Health Informatics Dr. David Soti, and the current head of the Division Dr. Peter Cherutich. We would also wish to acknowledge the technical coordination received from the Head of the e-Health Development Unit, Mr. Onesmus M. Kamau, who ensured the entire document development process was successful. We cannot forget the immense support received from Dr. Salim Hussein, the Head of the Community Health Services Unit at the Ministry of Health.

This document was developed and finalized through the financial and technical support of USAID MEASURE Evaluation-PIMA project and mHealth Kenya. Other support also came from the World Health Organization (WHO) and the Kenya Medical Research Institute-Wellcome Trust.

We recognize the expert contribution given by the Lead mHealth Experts Dr. Stephen Mburu of Modern Technology Computer Centre Ltd; Dr. Shem M. Angolo, Theo Computer Systems Ltd, Dr. Cathy W. Mwangi, mHealth Kenya; and Nancy Macharia of Samnet Communications Services Ltd. We also acknowledge valuable contribution by the Technical Review Committee comprising of Sophia Karanja, Gladys Echesa, Rachael Wanjiru, Nyokabi Njogu, Dr. Abel Nyakiogora and Diane Kamar of the Ministry of Health, Prof. Peter Waiganjo Wagacha of University of Nairobi, Prof. David Ngaruiya of International Leadership University, Willie Ngumi of GMSA, Joseph Mugah and Charles Mito of USAID MEASURE Evaluation PIMA, Steve Wanyee of Kenya Health Informatics Association (KEHIA), Dr. Doris Kirigia of KEMRI-Wellcome Trust, Ronald Osumba of ORACLE, and Dr. Geoffrey Wekesa Chcemwa of Jomo Kenyatta University of Agriculture & Technology who dedicated their time working as a team to ensure the successful finalization of this document. Last but not the least, is to recognize the role of Dr. Elisha O. Abade who led the process of developing this document.

TABLE OF CONTENTS

LIST OF TABLE AND FIGURES

LIST OF ABBREVIATIONS

API	Application Programming Interface
ASTM	American Society for Testing and Materials
CAK	Communications Authority of Kenya
CBO	Community-Based Organization
CCD	Continuity of Care Document
CDA	Clinical Document Architecture
CDC	Centers for Disease Control and Prevention
CEN	Comité Européen de Normalization
CHIS	Community Health Information System
DES	Data Encryption Standard
DFD	Data Flow Diagram
DHIS	District Health Information System
DSS	Decision Support System
DSTU	Draft Standards for Trial Use
EHEALTH	Electronic Health
EHR	Electronic Health Record
EMR	Electronic Medical Record
FBO	Faith- Based Organization
FHIR	Fast Health Interoperability Resources
FIT	Failure In Time
GSM	Global Systems for Mobile Communications
GUI	Graphical User Interface
HCI	Human Computer Interaction
HIE	Health Information Exchange
HL7	Health Level 7
HTML	Hypertext Mark-up Language
ICD 10	International Classification of Diseases revision 10
ICT	Information and Communications Technology
ICTA	Information and Communications Technology Authority
IDRC	International Development Research Center
IHE	Integrating the Health Enterprise
IRIs	Internationalized Resource Identifiers
ISMS	Information Security Management System
ISO	International Standards Organization
JKUAT	Jomo Kenyatta University of Agriculture & Technology
JSON	JavaScript Object Notation
KEBS	Kenya Bureau of Standards

KEMRI	Kenya Medical Research Institute
KEMRI-WT	Kenya Medical Research Institute-Wellcome Trust
KEMSA	Kenya Medical Supplies Authority
KMTC	Kenya Medical Training College
KNH	Kenyatta National Hospital
LIS	Laboratory Information System
LMIS	Logistics Management Information System
LOINC	Logical Observation Identifiers Names and Codes
M&E	Monitoring and Evaluation
MHealth	Mobile Health
MNO	Mobile Network Operator
MoH	Ministry of Health
MoICT	Ministry of ICT
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
NPHLS	National Public Health Laboratory Services
PEPFAR	President's Emergency Plan for AIDS Relief
PHI	Personal Health Information
PHR	Personal Health Record
PII	Personally Identifiable Information
PIS	Pharmaceutical Information System
REST	Representational State Transfer
SMS	Short Message Service
SNOMED	Systemized Nomenclature of Medicine
SOAP	Subjective Objective Assessment Plan
SRS	Software Requirements Specification
SSL	Secure Socket Layer
SW	Software
TBD	To Be Defined
TLS	Transport Layer Security
TTP	Trusted Third Party
UML	Unified Modelling Language
USAID	United States Agency for International Development
URL	Unified Resource Locator
WHO	World Health Organization
XDS-MS	Cross-Enterprise Sharing of Medical Summaries
XML	Extensible Mark-up language
XPHR	Exchange of Personal Health Record Content

DEFINITION OF TERMS

Authentication	A process of verifying the identity of entities (e.g. users) who try to access a system.
Client	A recipient of professional healthcare services.
Confidentiality	The degree to which access and disclosure of given information is limited to authorized entities (e.g. users) and for intended purposes only thereby preventing access by or disclosure to unauthorized entities (users).
Decision Support System (DSS)	An information system that supports decision making in an organization, hence a clinical DSS is an information system that processes clinical data and presents it so that users can make clinical decisions easily.
Developer Documentation	Documentation intended for use by software developers. It details the programming language specific constructs used in the software's source code.
Documentation	A write-up that describes, explains or instructs regarding some attributes of an object, system or procedure, such as its parts, assembly, installation, maintenance and use.
Drug House	A business involved in the manufacture, sale, or distribution of drugs.
e-Prescription	This is electronic writing and sending of prescriptions instead of using handwritten or faxed notes or calling in prescriptions.
Functional requirement	The specification of functions of a system, including the set of inputs and outputs of a system and its behaviour i.e. operations and activities that a system must be able to perform on the inputs before it delivers the outputs.
GUI	A short form of "Graphical User Interface" that refers to an interface that allows users to interact with the system through graphical icons and visual indicators rather than text alone. It typically comprises menu and forms that can be operated using mouse clicks or button/keypad events.

Healthcare service provider	An individual or an institution that provides preventive, curative, promotional, or rehabilitative health care services in a systematic way.
Implementers	A class of users who are involved in the development and delivery of the software solution.
Interoperability	The ability of two or more systems, services or products to work together or exchange information and correctly interpret the same without specific intervention by the user.
mHealth	Health services, interventions and/or programs accessed, delivered or availed through use of mobile technologies and devices.
Mobile Platform	An ecosystem of hardware, software and technology for laptops, tablets, mobile phones and other portable devices.
Non-functional Requirement	A requirement that specifies criteria for judging the operation of a system, rather than specific behaviours.
Pharmaceutical Technologist	This is a laboratory assistant or research assistant, usually a diploma holder, employed in the pharmaceutical industry under the direct supervision of a senior physician or scientist.
Pharmacist	A person licensed to prepare, compound and dispense drugs upon written order (prescription) from a licensed practitioner such as a physician, dentist, or advanced practice nurse.
Privacy	The aspect of information systems that deals with the ability that an organization or individual has to determine what data/information (about them) is to be shared with third parties.
Registered Premises	These are premises registered in accordance with section 23 of the Pharmacy and Poisons Act, and where a valid certificate for registration is available/has been issued.
Scalability	The ability of a computer application or product (hardware or software) to continue to function well when it (or its context) is changed in size or volume in order to meet user needs.

Security	The protection of information systems from theft, damage, alteration, exposure, disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting it against threats that may come via network access, data and code injection, or through malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures.
Usability	This is a measure the effectiveness, efficiency and quality of a system's interface with regard to a user satisfactorily performing a task.
Validation	The process of checking whether a product design or data input into a system satisfies the intended use. This can include checking the data type, syntax, data length, etc. Validation can be synchronous or asynchronous. ***Asynchronous validation:*** Validation that occurs after data has been loaded into the repository and that usually involves running of algorithms against data stored in the database to determine anomalies within the data. ***Synchronous Validation:*** Validation that occurs prior to the loading of data into the repository and that usually aims to verify that all data elements are reported using both a valid format and value.

1. INTRODUCTION

The Kenya Health Sector Strategic and Investment Plan (KHSSIP) 2014-2018 and Vision 2030 aim to support provision of "equitable, affordable and quality healthcare at the highest attainable standards" to all Kenyans. One of the key pillars of the KHSSIP is health information. This pillar aims to provide adequate evidence for decision making by consumers, policy makers and other actors in the health sector through one national integrated health information system. The integrated national health information system will be interoperable and will utilize different technologies. Technological innovations and mobile platforms will be used to achieve this vision. The Kenya mHealth Standards and Guidelines are aimed at guiding the utilization of wireless and mobile applications and devices to improve outcomes in health. This is also in line with the achievement of Vision 2030.

In Kenya, the use of mobile communication devices to deliver healthcare is gaining fast traction due to high mobile penetration and network coverage, hence, mHealth is one of the strategic areas of focus in the implementation of Kenya's e-Health Strategy 2016-2020. This encompasses telemedicine, health information systems, information for citizens (messaging services) and e-learning. Generally, mHealth has been defined differently by different groups and institutions: Some of the definitions are:

- **Foundation for the National Institutes of Health (FNIH)** - mHealth is "the delivery of healthcare services via mobile communication devices."
- **NIH Consensus Group** - "mHealth is the use of mobile and wireless devices to improve health outcomes, healthcare services and health research."
- **The mHealth Alliance** -"mHealth stands for mobile-based or mobile-enhanced solutions that deliver health."
- **US Broadband Plan** - "The use of mobile networks and devices in supporting e-care emphasizes leveraging health-focused applications on general-purpose tools such as smartphones and Short Message Service (SMS) messaging to drive active health participation by consumers and clinicians."
- **West Wireless Health**- "The delivery of healthcare services via mobile communication devices, such as cell phones. Applications range from targeted text messages to promote healthy behaviour to wide-scale alerts about disease outbreaks. The proliferation of cell phones across the globe, even in locales without basic healthcare infrastructure, is spurring the growth of mHealth in developing countries. Also known as mobile health."

- **World Health Organization (WHO)** -"Mobile Health (mHealth) is an area of electronic health (eHealth) and it is the provision of health services and information via mobile technologies such as mobile phones and Personal Digital Assistants (PDAs)."

- **Global Observatory for eHealth (Goe)** - "mHealth or mobile health is medical and public health practice supported by mobile devices, such as mobile phones, client monitoring devices, personal digital assistants (PDAs), and other wireless devices."

In general, mobile health (mHealth) refers to the use of portable devices such as cell phones to provide healthcare services and information. As mobiles and point-of-care devices become part of everyday life, people become better equipped to respond to primary care and emergencies through mobile applications such as remote patient monitoring.

In this document, the working definition of mHealth is interventions and programs designed to support health service provision through mobile technology and devices. The mHealth spectrum ranges from simple mobile phone-based applications for the transfer of health information on basic handsets via Short Message Service (SMS) to highly sophisticated diagnostic applications that rely on advanced equipment and robust back-end data systems. In Africa, most mHealth interventions, especially those targeting general populations, have used relatively simple mobile technology and equipment.

In many developing countries, much of the population, especially in rural areas, does not have access to the public healthcare system due to distance, resource constraints, system inefficiencies and a low awareness about services that are offered. Despite being in the embryonic stages, there have been promising early results and lessons from the dozens of mHealth pilot programs that have been conducted in a variety of geographical and health-system settings, many of which may be instructive in attempting to the addressed the needs.

1.1 Goal of mHealth Standards

The overall goal of mHealth standards in Kenya is to ensure the design, development and implementation of interoperable, scalable, sustainable mHealth solutions that benefit clients and healthcare workers in a cohesive and holistic manner for better health outcomes.

1.2 Purpose of mHealth Standards

These mHealth standards provide a regulatory framework that will enable coordination and implementation of robust mHealth solutions. The standardization will encompass communication protocols, device interfaces, applications and operating systems. This will support standards for information exchange to serve as the building blocks for the seamless

and secure exchange of health information for better and improved health service delivery and outcomes. Standardization further aims to move the mHealth sector from the silo-based pilot phases to scalable fully-fledged interoperable solutions.

1.3 Scope

The scope of these standards shall apply to both public and private sector stakeholders in the health sector, as described in chapter six of this document. The GSM Association generally categorizes mHealth solutions into two broad areas namely: solutions across the patient pathway; and healthcare systems strengthening.

Solutions across the patient pathway include wellness, prevention, diagnosis, treatment and monitoring all of which entail direct touch points with patients. Healthcare systems strengthening solutions on the other hand, include emergency response, healthcare practitioner support, healthcare surveillance and healthcare administration. These do not involve direct interactions with patients, but are primarily aimed at improving the efficiency of healthcare providers in delivering patient care.

The scope of these standards and guidelines will apply to both areas of mHealth to the extent that they handle Personal Health Information (PHI) and Personally Identifiable Information (PII). It shall apply to diagnosis, storage, analysis, and transfer using mobile systems.

1.4 Revision and Updates

These mHealth standards and guidelines shall be regarded as evolving entities, hence should be viewed as evolving guidelines. The standards may be reviewed for updates after every three years. The reasons for revision include policy change, upgrade of systems and any other changes in the operating environment.

2. DEVELOPMENT AND FUNCTIONS

This chapter describes the requirements that should be considered in the development, implementation, support, and maintenance of mHealth systems. The chapter also describes the functional and non-functional requirements of mHealth solutions. The application used should conform to WHO health informatics standards and other international standards, including among them ISO 9126-1 on software product quality and ISO 27799 on information security management in health.

The software development methodology shall be applied in consultation with the relevant stakeholders and shall include the following phases:

- Requirement gathering
- System analysis
- System design
- Development and implementation
- System testing
- Operations and maintenance
- Support
- Post-implementation monitoring and evaluation

The output of the above phases shall be validated by the production of the following documents:

i. Systems Requirements Specification (SRS)
ii. Software design documents: Depending on the software development methodology, the design documents will include any of the following:
    a. UML diagrams
    b. DFDs
    c. Flow charts
    d. Entity relationship diagrams
iii. Implementation plan: This shall include:
    a. Implementation manual
    b. Training and capacity building manual
iv. Test plans
v. Deployment procedures
vi. Monitoring and evaluation criteria

2.1 Documentation of mHealth System Development

The development of mHealth systems should be documented in order to facilitate continuity among the system users and developers. The mHealth system should have at least the following categories of documentation:

I. Technical manual
ii. Developer's guide
iii. User manual

These documents are essential for gathering details on the technical and functional specifications of the mHealth system. They can also be used to clarify and prioritize system requirements and to inform system design.

The target audience of each type of documentation is shown in Table 1 and details of each documentation are given in the sections that follow.

Table 2.1. Types of Documentation and their corresponding target audiences

Documentation Type	Target Audience
Technical manual	System administrators, system implementers
Developer guide	Programmers
User manual	System users

2.1.1 Technical Manual

The technical documentation should clearly outline the installation and maintenance processes of the system. This documentation should be thorough, but not so verbose that it becomes overly time-consuming or difficult to read and maintain. The technical documentation should specify:

i. Minimum hardware requirements: This should include the preferred hardware architecture, including memory and disk storage (internal and external) requirements.
ii. Minimum software requirements: This should include acceptable versions of the related software, including the minimum version of the underlying operating system.
iii. A list of software dependencies (external libraries) required for proper functioning of the system. This should clearly outline all pieces of software and correct versions that will be required for a successful installation and operation of the mHealth system.
iv. An installation guide that gives a step-by-step explanation of the installation process of the software. A graphical illustration of the installation process should be provided where possible.
v. A list of known and possible issues that might be encountered during the installation process and provide their corresponding solutions.
vi. The maintenance process of the system. In addition to being a separate document, this documentation should be preferably embedded in the system as a "README" file.
vii. Help line contact information with emails, Skype, and phone numbers of the person to be contacted for further help.

2.1.2 Developer's Guide

This class of documentation will be vital to software developers in the event of maintenance or modification of the mHealth system. It should provide an overview of the system, description of the software design methodologies, the system architecture and technical design diagrams of the system, among others. Typically, this class of documentation shall comprise the following:

i. User requirements analysis document
ii. System requirements specification document
iii. System design document (ERD,UML, DFD, Flow charts)
iv. Test documents (test plans, scripts and results)
v. Developer documents (source code documentation)

The overview of the system should include requirements documentation that outlines what the system does, summarizing or composed of requirements artefacts, such as business rule definitions, use cases, and essential data flows.

For database driven systems, this documentation should include:

i. Entity-Relationship Schema, including the following information and their clear definitions:
   - Entity sets and their attributes
   - Relationships and their attributes
   - Candidate keys for each entity set
   - Attribute and tuple-based constraints

ii. Relational Schema, including the following information:
   - Tables, attributes, and their properties
   - Views
   - Constraints, such as primary and foreign keys
   - Cardinality of referential constraints
   - Cascading policy for referential constraints
   - Primary keys

The system architecture should be easy to understand and not specific to the source code of the system. The source code of the system should be extensively documented. All the objects, classes, methods, functions and their associated parameters (where applicable depending on the system development methodology adopted) must be clearly described in the code comments.

2.1.3 User Manual

The user documentation should describe how the software is used within each feature of the system assisting users to understand how the system works. This documentation will include guide on how to run the system, how to enter data, how to update data and how to generate, save and print reports. The documentation should include a list of error messages and advice on what to do if something goes wrong.

The user manual must be organized in a manner such that the contents are easily accessible to the users. It is important to have a comprehensive "index" of the contents, organized alphabetically and easy to search. The documentation must be consistent and simple enough to understand by non-technical users.

This type of documentation will adopt any one of the following approaches (or a combination of two or more approaches):

i. **Tutorial:** The documentation that follows this approach will provide a step-by-step guide to the users on how to accomplish particular tasks within the system.
ii. **Thematic areas:** This kind of documentation should have chapters or sections that concentrate on one particular area of interest with respect to the various functionalities of the mHealth system.
iii. **List of references:** This refers to the approach in which the tasks or commands are listed alphabetically or logically grouped, often via cross-referenced indexes, in an organized manner.
iv. **Frequently Asked Questions (FAQ):** FAQ must provide a list of questions that are asked by most system users and will provide solutions to such common questions.

2.2 Minimum mHealth Functional Requirements

Different mHealth systems can be developed for different purposes and health settings, and therefore, may have different functions and capabilities. The mHealth systems range from client care systems to integrated commodity management. In order to maintain a core set of functions and encourage best practices, this section details the recommended functional requirements for mHealth systems, including recommended capabilities that are categorized into the following six classes:

1. Basic demographic data
2. Clinical decisions support
3. Automating simple tasks for health care providers
4. Health information and reporting
5. Product information
6. Health information exchange

2.2.1 Basic Demographic

The mHealth system should capture the following information where applicable:

- Name (First name and last name with an option for middle name or middle initial)
- Unique client identifier (should automatically be system generated)
- Date of birth
- Gender
- Next of kin
- Phone numbers
- Master facility list code
- Location

2.2.2 Clinical Decision Support

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

i. Highlight abnormal test results.
ii. Alert the provider about abnormal (outside the normal range) vital signs.
iii. Alert the provider about whether a known allergic drug is prescribed or if a known drug interaction is likely to occur.
iv. Provide notification of recommended care and treatment.
v. Support diagnostic and analytic functions.

2.2.3 Automating Tasks for Health Care Providers

Business Process Automation (BPA) is a strategy to contain or lower costs, which generally consists of application integration, reassigning labour resources and the use of software applications throughout the organization. Healthcare is arguably the only major industry in the world that hasn't embraced automation. One obvious and difficult result of this lack of automation is the worsening primary care provider shortage. Average wait times for a patient to get primary care are staggering. Process automation of healthcare solutions saves costs and increases the quality of standardized healthcare services. Some of the benefits that can be realized through automation are: labour savings, improved quality and consistency, reduced waste, increased predictability of outcomes, higher throughput, data driven insights.

2.2.4 Health Information and Reporting

To improve quality of service, mHealth systems should improve and promote the use of health information amongst users. They may be used to:

i. Generate reports from client data.
ii. Generate aggregate data in a standardized format for use at all levels.
iii. Reports generated from mHealth systems should be pushed automatically into the national reporting system.

2.2.5 Product Information

Inventory management using mHealth system should ease the capture the following information about the health-related products:

- Product code
- Product name
- Product version (where applicable)
- Date of manufacture
- Batch number (where applicable)
- Expiry date

2.2.6 Health Information Exchange

Health Information Exchange allows health care professionals and patients to appropriately access and securely share patient's vital medical information electronically. The demand for electronic health information exchange from one health care professional to another is growing along with efforts to improve the quality, safety and efficiency of health care delivery. Appropriate use, new payment approaches that stress care coordination, and financial incentives are all driving the interest and demand for health information exchange. Some of the benefits of HIE include:

- Providing a vehicle for improving quality and safety of patient care by reducing medication and medical errors.
- Stimulating consumer education and patients' involvement in their own health care
- Increases efficiency by eliminating unnecessary paperwork.
  Providing caregivers with clinical decision support tools for more effective care and treatment.
- Eliminating redundant or unnecessary testing.
- Improving public health reporting and monitoring.
- Creating a potential loop for feedback between health-related research and actual practice.
- Facilitating efficient deployment of emerging technologies and health care services.
- Providing the backbone of technical infrastructure for leverage by national and county-level initiatives.
- Providing a basic level of interoperability among Electronic Health Records (EHRs) maintained by individual clinicians and organizations.
- Reducing health related costs.

2.3 Minimum mHealth Non-Functional Requirements

Development process of mHealth applications is expected to conform to various non-functional requirements including:

1. Security
2. Interoperability
3. Scalability
4. Usability
5. Data validation

2.3.1 Security

The mHealth system must ensure that clients' data is handled in a secure manner by putting in place mechanisms that will guarantee privacy, confidentiality, integrity, availability and non-repudiation at all times. Thus, the systems must be secure from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording and destruction. The data must be secure both, in transit and when archived.

The general mHealth system security framework would entail the components described in Figure 2.1.

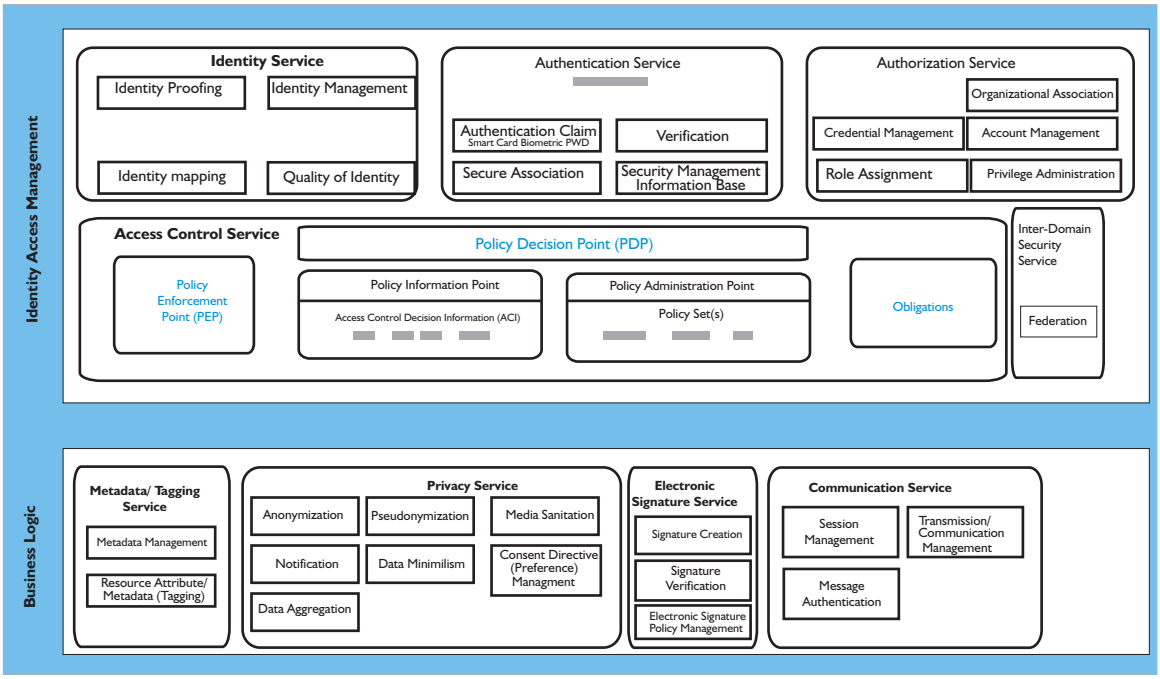


Figure 2.1. mHealth System Security Framework

2.3.1.1 Confidentiality

To guarantee confidentiality, the mHealth system must put in place measures to ensure that clients' data is protected against unintended or unauthorized access. The mHealth system shall:

i. Provide secure identity management services. This shall entail:
   a. Mechanisms for proving an entity's identity (that is, proving that an entity is who it claims to be), i.e. a secure authentication process.
   b. Mechanisms for unambiguously mapping an entity's submitted identity to the stored identity i.e. secure verification as part of the authentication process
   c. Mechanisms for monitoring the quality of identities submitted by entities e.g. the length and sophistication of a username and password for systems that use username/password authentication.

ii. Provide clear authorization mechanisms for access to sensitive data. Authorization for access to data should be based on need-to-know and least privilege policy. This should be dependent on information such as user identity, user role, location, sensitivity, type of data, date ranges covered by the data, author of the data, client identity, and client relationship to the user, client consent policies, time-of-day, purpose of use, and the workflow state.

The authorization module of the mHealth system shall, therefore, comprise of the following modules:

a. Credential management module
b. Role assignment module
c. Account management module
d. Privilege administration module
e. Organizational association module
f. Policy enforcement points (PEPs)
g. Policy decision points

iii. Use strong cryptographic technologies to ensure that clients' data is not stored in clear text format. The mHealth system shall use only the approved publicly known encryption algorithms, such as AES and RSA or a better algorithm. Weak encryption algorithms such as DES, and Triple DES (3DES) must not be used.

iv. Use hashing (one way functions) in conjunction with salting techniques to storing passwords of all users. Weak algorithms, such as MD5 or SHA1, must not be used.

v. Transmission of client data over the telecommunication networks for services such as web based information access, email, instant messaging voice of IP and internet faxing shall be secured using TLS/SSL. The use of TLS/SSL ensures that communications between a web browser and a server is private, the identity of the communicating parties can be authenticated and data integrity is assured, by use of digital certificates.

vi. Provide privacy services, including:

a. Anonymization of client data as much as possible before it can be shared
b. Where possible, use pseudonyms for the client data before it can be shared
c. Aggregate client data before it can be shared to reduce possibilities of tracing the data back to the client
d. Minimize data so that access is available only to the dataset required for that particular use

vii. Provide for communication management services including:

a. Session management service
b. Message authentication service

In addition, mHealth systems must comply with the provisions in the Kenya Health Bill 2015. More specifically, the following clauses of the Bill shall be adhered to:

i. Article 9 requiring the client's consent to be provided for health service.
ii. Article 10 on dissemination of health information by the national government, county governments and any other parties involved in provision of health services.
iii. Article 11 regarding confidentiality requirements pertaining to health information.

2.3.1.2 Integrity

The mHealth system shall ensure that clients' data is protected from alteration by unauthorized entities at all times, both during transmission and storage. To achieve this, the system must provide for:

i. Use of hashing techniques to monitor any changes in the data
ii. Use of cyclic redundancy checks (CRC) where applicable
iii. Use of checksums where applicable

2.3.1.3 Availability

The mHealth system shall put in place mechanisms to ensure that users can access and utilize the services provided by the system at all times and from anywhere. The mHealth system shall therefore exhibit attributes associated with maintaining high system availability, which include:

i. Allocating adequate storage and bandwidth capacity.
ii. Fast response time.
iii. Fast recovery capabilities.
iv. Performance monitoring.
v. Business continuity processes e.g. backups.
vi. Redundant sites and links.

The system availability shall be measured based on the following metrics:

i. Downtime per year: The mHealth application should have minimal downtime so as not to compromise its availability.
ii. Mean Time Between Failure (MTBF): The average time between failures in any of the mHealth system's modules must be guaranteed to be long enough to ensure that failures do not deny legitimate users access to the mHealth system.
iii. Mean Time To Repair (MTTR): Developers must ensure that it takes the shortest time possible to repair a failed module of the mHealth system, or, in the event that it is not practical to repair such modules within a short time, the developers must ensure that the mHealth system remains reliable.
iv. Failure In Time (FIT): This shall be measured by taking into account the number of failures in the mHealth system in a billion hours. This value should be kept at a minimum in order to guarantee availability of the system.

2.3.1.4 Non-Repudiation

The mHealth system shall put in place measures to ensure that actions or changes to data or components of the system shall be reliably associated with a unique user (individual), thereby ensuring that every user of the system cannot successfully refute or challenge any attempt to link them with the actions they have performed in the system. The mHealth system SHOULD achieve this by providing for:

i. Use of digital signatures for message authentication
ii. Authentication mechanism that is genuine and highly reliable
iii. Use of communication protocols that support digital certificates signed by trusted third parties (TTP)

iv. Implementation of audit trails for tracking the origin, authorship, history, status, and accessibility of information

In addition to putting in place the technical requirements above, the mHealth system should conform to the following guidelines:

1. Only collect health information that is needed for the purpose for which it was designed.
2. Get the information directly from the people concerned.
3. Tell the providers of the information what you are going to do with the information.
4. Be considerate when collecting the information, keeping in mind the clients right to privacy.
5. Take care of the information once it is received.
6. Ensure that people can see their health information if they choose to.
7. Ensure that people can correct their health information if it is erroneous.
8. Make sure that the health information is accurate before it is used.
9. Discard or securely put away the client's health information when the session or instance is over.
10. Use people's information strictly for the purpose for which it was intended.
11. Only disclose the information if there is a good reason to do so and in accordance with the provisions of the Kenya Health Bill 2015, Articles 10 and 11.
12. Only assign unique identifiers, where permitted, and in accordance with Section 1.3 of the Kenya Interoperability Standards and Guidelines 2015.
13. Where patient level data is required to be shared for non-clinical and patient management purposes, it must be de-identified. This involves determining the sensitive fields in the client's data, then ensuring that these fields are removed, obscured or obfuscated so that the remaining information does not identify an individual. This can be achieved using a code, algorithm, or pseudonym that is assigned to individual records.
14. Where patient data needs to be used for decision making, research, national requirements and policy formulation, the data should be given as aggregates to the extent possible.
15. The process of data archiving should be in accordance with the Kenya Archive Act, research protocols where applicable, and the eHealth policy on management of health data.
16. Subscribers /users of the mHealth system shall be provided with the option to unsubscribe from the system whenever they desire to do so.
17. Program managers working with application developers are expected to define and implement a reasonable retention period for data collected with the application and predefine a period of inactivity after which the account will be treated as expired.

2.3.2 Interoperability

There are primary information systems used for data capture, reporting and decision support in various domains of the health sector. The mHealth system must provide for seamless integration with these systems by incorporating at minimum the following types of interoperability:

- Technical interoperability
- Semantic interoperability
- Process interoperability

Further, the mHealth system must comply with the interoperability requirements as outlined in Chapter 3 of this standard.

2.3.3 Scalability

The mHealth system shall be designed to support increased workload by accommodating increased traffic, number of users, number of datasets, size of the database, etc. The mHealth system design shall address scalability requirements by embedding features, such as:

i. Designing for fault tolerance by providing for load balancing, load monitoring, and self-healing;
ii. Statelessness: Only minimal (or none at all) system state information should be maintained by the application server in memory;
iii. Limited sharing of resources to the database only;
iv. Offering in-memory distributed caching to reduce the number of actual database access; this will limit pressure put on the storage devices;
v. Use of database replication and partitioning;

2.3.4 Usability

Usability of the system should be enhanced by taking into account the socio economic status of the targeted users. Therefore, mHealth systems should:

I. Be easy to install - the installation process should be simple and well-documented.
ii. Be easy to update - this process should be simple and well-documented and to the extent possible, the updates should be seamless, automated and centrally managed.
iii. Be intuitive - the system's user interface design should be well thought-out and gauged to meet the interests and abilities of the intended users.
iv. Be efficient - the system should be fully optimized for the specific architecture on which it runs. It should not result in memory leaks or any form of over utilization of shared resources. It should work seamlessly with the underlying structures and subsystems.
v. Be pleasant and easy to navigate - the look and feel of the system's interface should be well thought out based on "what works" for the specific device and architecture rather than on "what is trending".
vi. Be easy to exit either by uninstalling or unsubscribing – the procedure for exiting should be simple and clearly documented.
vii. Have minimal dependency on third party software, and where such dependency is inevitable, it should be well documented and packaged with the software. The dependencies must also be installed as part of the installation process.
viii. Be easy to troubleshoot – the system must allow for simple ways of investigating the root causes of problems when the system fails.
ix. Have effective error handling – when the system comes across an error, it should make the error known to the user (and to the developers). In the event of an error, the system should warn the user, attempt to rectify the error and provide options of reporting the error to the developers.
x. The user system should allow for multilingual installation on a single application.

2.3.5 Data Validation

The mHealth application must provide mechanisms for validating data during data entry at source to ensure that data collected and processed is accurate, reliable, in the right format and organized in a way that assures credibility for reporting and evaluation. The mHealth system, therefore, should exhibit both synchronous and asynchronous data validation approaches by enforcing the following controls in order to ensure proper validation of data:

i. Ensure that data is accurately typed at all times (i.e. the correct data type is adhered to at all times).
ii. Data length is checked and field's length minimized.
iii. Range is checked for all numeric data.
iv. For all numeric fields, the value entered is unsigned unless that field is explicitly required to have a signed value.
v. Sanitize any input data before submission to the database.
vi. Apply good practices of URL encoding and HTML encoding where applicable.
vii. Use the XML functions to validate XML input.

The following are levels of data validation that must be supported by all mHealth Systems:

i. First Order Validation
   - Ensure that data elements are in valid format and value
   - Prevents obvious data entry errors

ii. Second Order Validation
   - Historical comparison for the same data so that an alert is prompted if an indicator increases or decreases

iii. Third Order Validation
   - Assess data elements for consistency within specific form or set of indicators

iv. Fourth Order Validation
   - Assessment of any statistical outliers (which may or may not be accurate)

3. INFORMATION EXCHANGE – INTEROPERABILITY

In different domains of the health sector, there are primary information systems used for data capturing, reporting and decision support. Developers of mHealth applications must identify the domain of operation and the existing standard reporting and decision support systems within the domain, identify and implement requisite requirements for health information exchange. Currently, the following are some of the information management systems used in health domain:

- Community Health Information System (CHIS)
- District Health Information System (DHIS2)
- Laboratory Information System (LIS)
- Logistics Management Information System (LMIS)
- Pharmaceutical Information System (PIS)
- Electronic Medical Records (EMR)
- Electronic Health Records (EHR)

The mHealth development process should take into account the sharing of information and integration of related data in such existing application(s), including other social determinants of health. To enable the integration of mHealth solutions and the existing health information systems, the developer should ensure that they incorporate in their design the following levels of Maturity Interoperability Model shown in Figure 3.1:

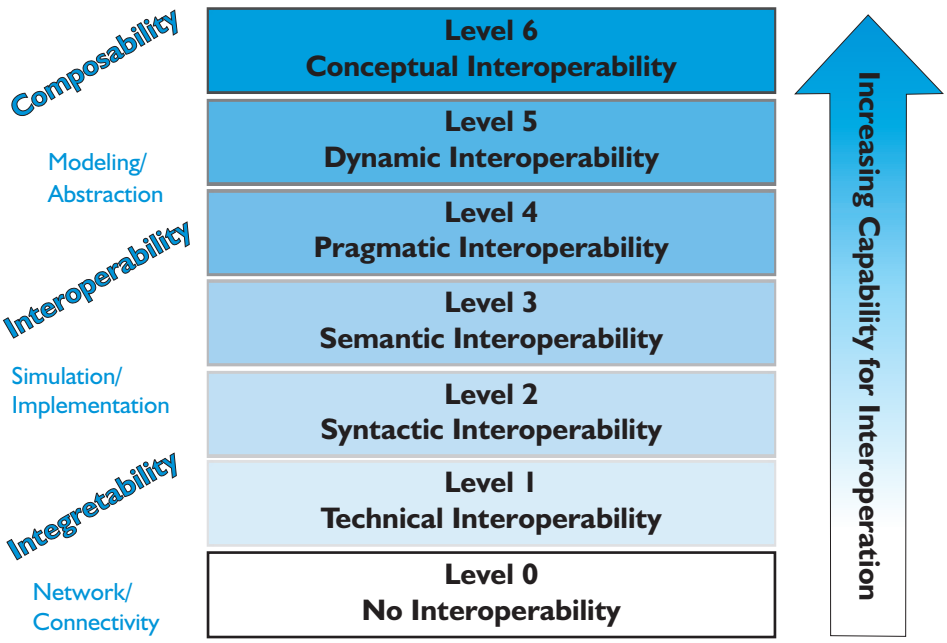


Figure 3.1: Conceptual interoperability maturity framework

- Maturity level 0: No maturity whatsoever therefore this level should be ignored
- Maturity level 1: Integration or technical interoperability
- Maturity level 2: Syntactic and workflow interoperability (this includes integration)
- Maturity level 3: Semantic interoperability (this includes both integration and workflow)
- Maturity level 4: Pragmatic interoperability (this includes all of the above with a dash of Artificial Intelligence (AI)
- Maturity level 5: Dynamic Interoperability – as a system operates on data over time, the state of that system will change, and this includes the assumptions and constraints that affect its data interchange. If systems have attained Dynamic Interoperability, they are able to comprehend the state changes that occur in the assumptions and constraints that each is making over time, and they are able to take advantage of those changes. When interested specifically in the effects of operations, this becomes increasingly important; the effect of the information exchange within the participating systems is unambiguously defined.
- Maturity level 6: Conceptual Interoperability – this requires that conceptual models are documented based on engineering methods enabling their interpretation and evaluation by other engineers. In essence, this requires a "fully specified, but implementation independent model"

The mHealth system must conform to the interoperability requirements as outlined in the Kenya Interoperability Standards and Guidelines. Specifically, the mHealth application must conform to:

i. Section 1.0, which describes the acceptable data exchange standards for terminology, messaging and documentation
ii. Section 1.1, which outlines methods of exchange and specifies automated methods, such as use of "middleware" or API-based recognized formats, including JSON and XML
iii. Section 1.2, which describes data types and units of measure that should be internationally accepted domain specific units
iv. Section 1.3 on unique identifiers for clients, facilities, health care professionals and non-medical institutions

The mHealth application interoperability must also be compatible with the recommendations made in internationally accepted standards, namely:

i. Clinical Messaging - the system must conform to Health Level 7 version 3 (HL7 v3) standards and its corresponding implementation guideline specifically, the system must conform to the requirements outlined in section 6 of the HL7 v3 standard on naming conventions. This section gives guidelines on naming conventions, including Internationalized Resource Identifiers (IRIs), class naming, property naming and ontology naming and versioning.

ii. Clinical Terminology – terminologies and classifications for clinical concepts, such as diseases and medications, must conform to international standards, including:
    - International Classification of Diseases revision 10 (ICD 10) – for diseases

- Systemized Nomenclature of Medicine (SNOMED) – for clinical data coding
- Logical Observation Identifiers Names and Codes (LOINC) – for laboratories
- RxNorm – for Pharmacies

iii. The system must use the latest versions of these international standards.

- Documents – where mHealth system needs to indicate the type of information included in a document and also the location of the information, this must be done in accordance with the accepted international standards. The applicable standards will be paper-based Subjective, Objective, Assessment, Plan (SOAP), HL7 Clinical Document Architecture (CDA) for electronic sharing of clinical documents, (HL7 CCD) and a discharge summary (HL7 DS).
- Health Level 7 Clinical Data Architecture (HL7 CDA) is an XML-based, electronic standard used for clinical document exchange and conforms to the HL7 V3 Implementation Technology Specification (ITS). It is based on the HL7 Reference Information Model (RIM), and uses HL7 V3 data types.
- Health Level 7 Continuity of Care Document (HL7 CCD) is a standard built on HL7 CDA to cater for compatibility with the ASTM Continuity of Care Records (ASTM CCR) standards and uses a detailed set of constraints (templates) for CDA elements to define how to use the CDA elements to communicate clinical data.

iv. Concepts – to allow for transmission of information between systems without any loss of the meaning or context of that information, the mHealth systems will adopt the notion of "concepts". The applicable standard for the implementation of concepts shall be Health Level 7 Reference Implementation Model (HL7 RIM) or any other appropriat standards. In HL7 RIM, concepts are defined based on the following five Modelling facets:

a. Act
b. ActRelationship
c. Participation
d. Roles
e. Entities

In the HL7 RIM approach, every happening is an Act e.g. procedures, observations, medications, supplies, registration, etc. Acts are related through an ActRelationship. This can be composition, preconditions, revisions, support, etc. Participation defines the context for an Act, such as the author, performer, subject or location. The participants are Roles e.g. client, provider, practitioner, specimen, or employee. Roles are played by Entities, such as persons, organizations, material, places, devices, etc.

v. Architecture - mHealth systems developers will be required to provide the system architecture that defines a generic model of the system, thereby providing

data elements and the business logic of the system. The architecture should cover all the three viewpoints of the system, including enterprise viewpoint, information viewpoint and computational viewpoint. The applicable standards for this shall be adopted from Standard Architecture for Information Systems (ENV 12967) developed by European Committee for Standardization (CEN).

3.1 API Interoperability

Developers of mHealth solutions shall provide Application Programming Interfaces (APIs) that define how they interact with other systems. The applicable API interoperability standard shall be Fast Health Interoperability Resources (FHIR). The FHIR API exposes FHIR resources using a Representational State Transfer (REST) based approach to access clinical, administrative, and infrastructure data. The API supports a consistent set of interactions across all resource types, including search, read, create, update, and delete. The figure below illustrates the FHIR architectural framework.

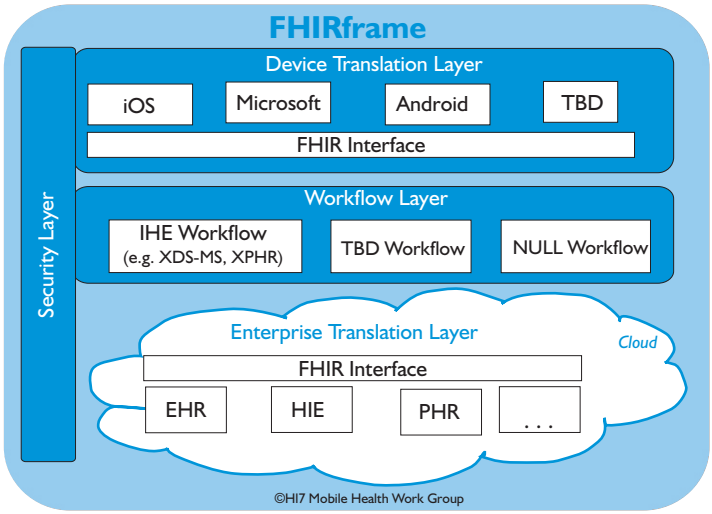


Figure 3.2: Fast Health Interoperability Resources Framework

The FHIR architecture consists of several layers. The device translation layer consists of software for interfacing between various medical devices and mobile platforms. The IHE domain workflow layer contains software that ensures that IHE workflows are followed while the enterprise translation layer consists of software that interfaces to EHRs. The security layer provides software that ensures secure transmission of data. FHIR provides guaranteed interoperability by adopting all the four paradigms of interoperability and its APIs meet IHE and HL7 standards. The supported paradigms are:

i. RESTful web services
ii. Documents
iii. Messages
iv. Services

4. DIGITAL MESSAGING AND E-PRESCRIPTION

4.1 Standards for Short Messaging Service (Texting)

Sending text messages using Short Message Service (SMS) can be useful means of communication especially in low-resource settings. However, if it is done without adequate safeguards can expose an organization to potential privacy and confidentiality violation.

4.1.1 Risks of Texting Personal Health Information

Some of the limitations of using SMS as means of transmitting health data and information include:

i. Lack encryption on SMS messages transmitted via mobile cellular network control channel
ii. The sender does not know with certainty that his/her message is indeed received by intended recipient
iii. Telecommunication vendors may read stored SMS messages

4.1.2 Proposed Standard for Texting in Healthcare

i. DECIDE: Decide whether mobile devices will be used to access, receive, transmit or store patients' health information or be used as part of your organization's internal network or systems.
ii. ASSESS: Consider the risks when using mobile devices to transmit the health information your organization holds.
iii. IDENTIFY: Identify a mobile device risk management strategy, including privacy and security safeguards.
iv. DEVELOP: Develop document and implement mobile device policies and procedures to safeguard health information.
v. TRAIN: Conduct mobile device, privacy and security awareness and trainings for consumers, healthcare providers and ICT professionals.

4.1.3 Guidelines to Help Secure Patient Health Information

i. Install and enable encryption to protect health information stored or sent by mobile devices.
ii. Use strong password or other user authentication.
iii. Install and activate wiping and/or remote disabling to erase the data on your mobile device if it is lost or stolen.
iv. Disable and do not install or use file sharing applications.
v. Install and enable a firewall to block unauthorized access.
vi. Install and enable security software to protect against malicious applications, viruses, spyware, and malware-based attacks.

vii. Keep your security software up to date.
viii. Research on mobile applications (apps) before downloading.
ix. Maintain physical control of your mobile device. Know where it is at all times to limit the risk of unauthorized use.
x. Use adequate security to send or receive health information over insecure wireless networks.
xi. Delete all stored health information on mobile device before disposal.

4.1.4 Overall Risk Management Strategy

i. Banning the texting entirely, limiting the texting of identifiers, diagnosis and other information.
ii. Setting policies that require deletion of texts.
iii. Passcode protection
iv. Encryption
v. Secure disposal of devices
vi. Registration of devices including personally owned.
vii. Use of 3rd Party Secure Messaging Solution.

4.2 Standards for electronic consultation and prescription

4.2.1 Mobile or telephone-based consultations

This standard defines technology-based patient consultations as the process of electronic interaction between a client and a healthcare provider using any form of technology, including, but not limited to interactive voice and video response (IVVR), videoconferencing, mobile voice calls, Voice over internet protocol (VOiP), and SMS-based messaging.

4.2.2 Good Medical Practice

Good medical practices to be considered before deploying or use of technology-based interactions are as follows:

- Certified health care workers have a duty to make the care of patients their first concern and to practise medicine safely and effectively. They must be ethical and trustworthy.
- Certified health care workers have a responsibility to contribute to the effectiveness and efficiency of the health care system. It is important to use health care resources wisely, ensuring that the services provided are necessary and likely to benefit the patient regardless of the circumstances in which they consult a patient.
- It is equally valid for technology-based patient consultations as it is for traditional face-to-face interactions.

4.2.3 Providing technology-based patient interactions

Healthcare providers and/or practitioners who advise or treat patients in technology-based patient interaction should adhere to the following guidelines:

1. Apply the usual principles for obtaining their patient's informed consent, protecting their patient's privacy and protecting their patient's rights to confidentially
2. Make informed judgement about the appropriateness of a technology-based patient consultation and in particular, whether a direct physical examination is necessary
3. Fully identify themselves to the patient or subject of care
4. Confirm to their satisfaction the identity of the patient at each consultation. Health providers should be aware that it may be difficult to ensure unequivocal verification of the identity of the patient in these circumstances
5. Provide an explanation to the patient of the particular process involved in the technology-based patient consultation
6. Ensure they have mutual communication with the patient/subject of care to:
    a. establish the patient's current medical condition and past medical history, and current or recent use of medications, including non-prescription medications
    b. identify the likely cause of the patient's condition
    c. ensure that there is sufficient clinical justification for the proposed treatment
    d. ensure that the proposed treatment is not contra-indicated. This particularly applies to technology-based consultations when the practitioner has no prior knowledge or understanding of the patient's condition(s) and medical history or access to their medical records
7. Accept ultimate responsibility for evaluating information used in examination/diagnosis and treatment subject to verification with the source. This applies to information gathered by a third party who may have taken a history from, or examined, the patient
8. Make appropriate arrangements to follow the progress of the patient and inform the patient's general practitioner or other relevant practitioners
9. Keep an appropriate record of the consultation

4.2.4 Emergency Situations

In emergency cases, it may not be possible to practise according to these guidelines. If an alternative is not available, a technology-based client consultation should be as thorough as possible and lead to more suitable arrangements for the continuing care and follow up of the patient.

4.2.5 Digital Delivery of Prescriptions

Digital prescriptions (e-prescription) within a formally defined order entry and prescription framework is the process of electronically prescribing and transmitting a prescription order to a certified healthcare provider (pharmacist or pharmaceutical technologist) to dispense

prescribed drugs to a client. This is done to among other reason; to improve accuracy, enhance patient safety, quality of care and continuity of care for individual patients.

4.2.6 Using electronic prescriptions

The client has the right to choose to which pharmacy where their prescriptions shall be delivered electronically. This will normally be through a registered pharmacy or chemist, manned by a qualified and registered pharmacist or pharmaceutical technologist. This guideline mandates the patient to have the right to change or cancel the nominated pharmacy or chemist at any time and the following must be observed

- Patient must be fully informed about the electronic prescribing system before the pharmacy or chemist of choice is set on the system
- Patients have the right to opt-in or out and no changes to the pharmacy or chemist of choice can be made without the patient's consent
- All prescription authorizations transmitted electronically must originate with the prescriber and be sent directly from a device authorized by the prescriber.

4.2.7 Authentication of Prescriptions

Medical prescription delivered electronically has to be from an authorized and licensed medical practitioner. All prescriptions dispensed electronically must bear the professional's practising license number issued by relevant licensing bodies. It is the responsibility of the drug dispenser to authenticate and validate the prescription prior to dispensing the medication. Narcotics, controlled drugs and targeted substances must not be prescribed electronically.

Regular SMS messaging is not considered equivalent to receiving a digital prescription, but may be used as a medium to notify the pharmacy to log in to the application to view the prescription. The prescription should be delivered using secure transmission channels and protocols and NOT on protocols such as SMS that send unencrypted messages. For any prescription received through a mobile platform, pharmacists or pharmaceutical technologist(s) must observe the following:

1. The process of receiving e-prescriptions must maintain patient privacy and confidentiality. The application receiving the prescription must be within a secure area where the transmission is received and handled only by pharmacy staff, to protect the confidentiality of patient information.
2. If any document containing personal health information is received in error, the pharmacy should notify the sender that the electronic prescription was received in error and destroy the information in a secure manner.
3. Patient choice must be protected; that is the patient must determine the pharmacy where the prescription is to be dispensed.
4. The patient has a right to receive a copy of the electronic prescription from the dispensing pharmacy either in hardy copy or electronic format

4.2.8 Delivery of Electronic Prescribed Drugs

The delivery of electronically prescribed drugs must always be dispensed by a qualified and licensed pharmacist or pharmaceutical technologist and in a registered premises. Thus, once a prescription is electronically sent, the patient must physically collect the drug from the nominated outlet.

4.2.9 Digital prescribing Dataset

The following is a list of attributes that are required to identify each patient in a typical e-prescription dataset:

Minimum demographics attributes for e-Prescription

- Surname
- Given name
- Date of birth
- Unique Personal identifier
- Gender

Prescription authentication

- Prescription ID
- Issue date
- Identity of health service provider
- Professional qualifications
- Phone contact of health service provider
- Work address
- Practicing license number
- Digital signature of health service provider

Prescribed Product Identification

- Name of the product (identifier)
- Strength of the product
- Prescription information
- Pharmaceutical dosage
- Quantity
- Dose regimen
- Duration of treatment (start and/or stop time)
- Directions for use
- Pharmaceutical preparation description

5. IMPLEMENTING mHEALTH SYSTEMS

The implementation process of mHealth system shall entail the following phases: planning; designing; monitoring and evaluation; and scaling up. It requires careful and well thought-out planning facets for example, knowledgeable people who know how to use the system, operationalized design documents, technical support and monitoring and evaluation of progress, outputs, outcomes and impacts. Figure 4 illustrates the elements of mHealth system implementation.

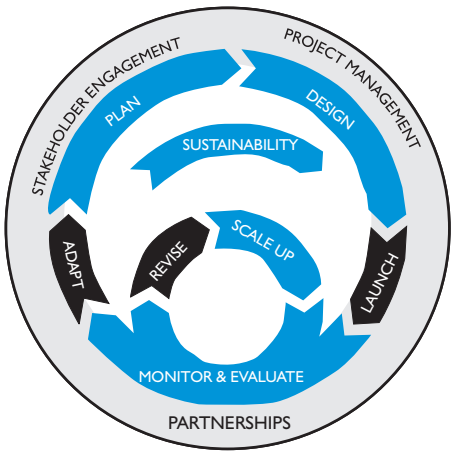


Figure 5.1: mHealth implementation schematic

5.1 Planning

The planning phase in the implementation of mHealth system shall require:

i. A comprehensive landscape analysis
ii. Identification of local and national priority health needs
iii. A comprehensive target audience analysis
iv. Project management skills with respect to people, systems and data
v. Partnership analyses and development

5.1.1 Landscape Analysis

In planning for the implementation of mHealth systems, a comprehensive landscape analysis must be undertaken. As a guideline, landscape analysis shall include:

i. Analysis of the country's mobile phone market penetration. This will include the following aspects, among others:
    a. Urban/rural penetration
    b. Sex (male/female)
    c. Type of phone: basic phone/Smartphone
    d. Carrier/platform use
    e. Projections on how the penetration would change with time

ii. Analysis of local and national priority target health needs and expectations that are measurable and evaluated.
iii. Analysis of the key players in the mobile industry, such as Mobile Network Operators (MNOs), telecommunication regulators, aggregators and handset manufacturers.
iv. Analysis of the current mobile market trends and drivers and how these will change in the near future.
v. Analysis of current mobile industry regulations, policies, and upcoming changes.
vi. Analysis of the average monthly mobile phone expenditure for the proposed target population.
vii. Analysis of the average total cost of mobile phone ownership for an individual in the target population and whether it is decreasing, increasing, or staying the same.
viii. Analysis of the telecom market advances that are driving the cost structure for users and how these will possibly impact the uptake of the mHealth solution
ix. Analysis of how the target audience uses mobile phone services.
x. Analysis of whether there are similar or complementary mHealth solutions that exist in the country, particularly in the geographical location you would like to target.
xi. Analysis of applicable technological platforms that will be required especially if the mHealth solution will be developed from scratch.

5.1.2 Local and National Priority Health Needs

The Kenya Health Policy and related documents has recognized the following as priorities to attainment of the highest standard of health and wellbeing:

i. Elimination of communicable conditions by reducing the burden of communicable and non-communicable diseases
ii. Reduction of the burden of violence and injuries by putting in place strategies that address the causes of injuries and violence.
iii. Provision of essential healthcare services and information using equipment and resources that are affordable, equitable, accessible and responsive to client's needs.
iv. Minimizing exposure to health risk factors through strengthening and promotion of health interventions such as that lead to health seeking behaviour.
v. Strengthen collaboration to ensuring the players in the health sector influences design, implementation and monitoring of health related interventions and actions.

5.1.3 Target Audience Analysis

Planning for the implementation of the mHealth system shall include understanding the audience that will use the proposed solution. Analyses of the target audience will include:

i. Describing the current technological access and practices of the end users. A basic guideline on the aspects of analyses shall include:

a. Whether individuals in the target population currently own mobile phones or share phones with others.
b. Whether the level of mobile phone ownership is influenced by gender
c. The type of phones that members of the target population use (basic, feature phones or Smartphones)
d. Who pays for the phone and airtime and whether costs affect their use choices and patterns (e.g. SMS, "please call me" etc)
e. Average duration of maintaining same phone numbers
f. The average number of SIM cards owned by the target audience and how often they switch between numbers
g. How the people in the target audience recharge their devices and how long they go without recharging their phones

ii. Analysis of the target population's health needs and its perception of health solutions
iii. If applicable, cultural and gender dynamics around the health issues and/or mobile phone use

5.1.4 Project Management

Planning for the implementation of mHealth systems shall entail an adoption of sound project management practices encompassing people, systems and data.

5.1.4.1 People

i. Ensuring that there is a project manager who possesses key attributes needed to successfully manage the mHealth program
ii. Putting in place a well-defined implementation team
iii. Clearly defining the roles and responsibilities of members of the implementing team and the partners
iv. Ensuring that the roles and responsibilities of the implementation team and partners are clearly communicated to each individual

5.1.4.2 Systems

With respect to systems, the following measures should be considered:

i. Updating of organizational policies and procedures to support the mHealth system
ii. Training of staff members and/or end users on how to implement the mHealth system
iii. Building the capacity of the target population to ensure informed participation throughout the formulation, implementation and monitoring and evaluation of the system
iv. Putting in place mechanisms for regular communication between the technological partners, other stakeholders and the mHealth system implementer
v. Putting in place mechanisms to ensure that the project team members keep each other accountable to the work plan, timeline, and budget

vi. Putting in place supportive supervision mechanisms to help staff implement and manage the change in practice that will arise due to adoption of the mHealth system
vii. Training of supervisors, not only on the technology and content of the mHealth system, but also on how to manage staff and user challenges that will arise during the implementation process
viii. Putting in place mechanisms for monitoring the effects of the mHealth system on staff workload and workplace procedures and processes

5.1.4.3 Data

The data aspect of program management should clearly define policies and procedures that will include:

i. A plan for collecting and tracking cost data
ii. A plan for collecting and tracking user data
iii. A plan on how the lessons learnt will be documented and shared with the implementing team and other partners
iv. A plan on how these lessons will be shared with the larger mHealth community
v. A plan to ensure consent is sought from the target population and data confidentiality issues are addressed prior to the utilization of the data

5.1.5 Partnership Development

The successful implementation of mHealth system will require partnerships with different stakeholders, as explained in chapter 6 of this standards document. This partnership development shall be achieved by:

i. Ensuring that all the relevant parties are brought on board at the implementation stage
ii. Providing incentives to users and implementers of the mHealth system for their participation
iii. Ensuring that roles and responsibilities of each partner/stakeholder are clearly defined and understood by all
iv. Drawbacks, if any, of the partnership should be identified and communicated
v. All stakeholders should truly understand and support the proposed project goals and objectives
vi. The benefits and potential (scale, sustainability) of the mHealth solution for each group of stakeholders are identified and articulated to stakeholders
vii. Analyzing the partnership relationship to see how it will change over time
viii. Addressing and resolving all stakeholder concerns as they arise

5.2 Designing

Design is a key component of the mHealth system's implementation. A proper mHealth implementation design must reflect design options with respect to:

i. Technology design decisions

ii. Content development and testing
iii. Prototyping and usability testing
iv. Usability decisions and user centric design and development
v. Improved work flow and reduced burden of use
vi. Value addition from the current set of tools

5.2.1 Technology Decisions

Successful implementation of mHealth systems will require analyses on various technological issues, including:

i. Core functionality of the system
ii. Data analytics, storage and availability
iii. Security, hosting and privacy
iv. Mobile delivery platform
v. Monitoring and maintenance
vi. User considerations – hardware, equipment, power and connectivity needs
vii. Enabling environment – regulations, national policies and interoperability
viii. Integration potential
ix. Scalability
x. Sustainability
xi. Licensing

5.2.2 Creation of Message Content

Development of SMS message for mHealth systems must be informed by preferences and abilities of the target audience. The following considerations should be made during content development:

i. Language - the mHealth system should be implemented in a language that will be clearly understood by the target audience.
ii. Vocabulary and phrasing- the system must use typical words or phrases that the target audiences uses to talk about their health issues
iii. Length - the system design should consider how long each message or screen should be bearing in mind the attention span of the target audience and ease of use
iv. Frequency and timing - the delivery of content to the audience must consider how often the messages or content should be sent or received by the audience and preferred time of receipt of the messages. Implementation must consider user preferences for receiving and sharing information.
v. Tone – for each message content, the implementer must consider the tone (informal, colloquial, professional, and technical) that would resonate most with the end users
vi. Messenger – the implementer should consider whether and how the source or perceived source of the message will influence a user's reaction to the content
vii. Accuracy – the content must adhere to the country's technical guidelines and international standards
viii. Consistency – if the mHealth solution is part of a multi-channel campaign, the

messages must be consistent and complementary across the program

ix. The messages should be approved by the relevant ministry of health authorities. The SMS context and content used in the mHealth System is owned in trust by the Government of Kenya.

5.2.3 Testing of Message Content

After developing the content, the following testing criteria can be used:

i. Test all of the messages or content, one section at a time, in the intended sequence and format
ii. Ask a number of probing questions to assess the user's ability to understand, remember, and/or react to the message
iii. Observe the participant's verbal and non-verbal cues, noting moments of confusion or pause as well as ease
iv. Ask the users how easy or difficult they find the messages
v. Explore reactions to, and preferences for, content length, tone, frequency, and the messenger
vi. Ask for suggestions for word choice, key words, or visuals for multimedia messages

5.2.4 Prototyping and Usability Testing

Before actual deployment of any mHealth system, the artefact should first be implemented as a prototype, released in a beta version and tested with a small number of users for feedback in order to confirm its usability, identify and fix bugs, and improve its overall functionality. The general rule of thumb is that implementation should start with a small group as possible with minimal costs, and then continue to be tested, improved, and iterated. During this phase, the following issues should be considered:

i. Whether the solution functions as intended, and if not, identifying what does or does not work well
ii. What the end users like and dislike about the solution and clearly outlining aspects that could be improved and how they could be improved
iii. Whether the end users are interacting with the technology as expected
iv. Whether the end users understand the content
v. The preferences of the end users for when and how often to be contacted
vi. Whether the project administrators find the technology platform easy to use and clearly documenting what they like or dislike about the administrative user interface and what improvements can be made
vii. Whether data is collected as intended and is in the correct format
viii. The anticipated barriers to correct use, based on observation and user feedbacks

5.3 System Launch

A launch plan for the mHealth system should consider best practices that include:

i. Launching in beta version

ii. Coming up with creative ways of generating demand for use of the mHealth solution
iii. Capacity building to ensure proper usage.
iv. Clearly communicating the advantages of using the application, such as efficiency and improved work flows

5.3.1 Launching the Beta Version

For mHealth systems developed from scratch, it is recommended that they are initially released as beta versions so as to help the implementers consider elements that need to be tested before a scale- up. To realize this, the implementers must:

i. Make a list of what can go wrong that would have a large impact on the user experience and program operations, and ensure that these functions can be tested and managed and that bugs are resolved during beta testing
ii. Determine who the audience for beta testing will be
iii. Develop and implement a training plan and a communication plan
iv. Determine how data will be collected from the beta testing audience and addressed before the launch to a wider audience
v. Show how much time will be needed to do the beta testing to ensure that a product does not remain in the beta phase forever

5.3.2 Generating Demand for the System

The mHealth system implementation plan must provide the following procedures and instructions:

i. How the potential end users will find out about the mHealth system.
ii. How the awareness generation activities will be tested and detailing the anticipated rate of conversion to use after awareness creation activities are conducted.
iii. Stakeholders who act as champions in awareness creation for mHealth systems among implementers and end users
iv. The incentives and benefits for those implementing the mHealth system.
v. The incentives and benefits for the end users of the mHealth system.

5.3.3 Training and Supportive Supervision

Training and supportive supervision must be monitored as part of the mHealth system's deployment process to ensure that everyone understands:

i. The rationale behind the implementation of the mHealth system.
ii. Policy or procedural changes that will take place to accommodate the mHealth system.
iii. Instruction on how to use the mobile device and application (if applicable).
iv. How to report and operate around implementation challenges.
v. Data management and use.
vi. The opportunity for those who will be affected by the changes to ask questions and express concerns about the process.

The mHealth training and support supervision plan shall provide the following guidelines:

i. Describe the training program that will be implemented before the launch.
ii. Describe the opportunities for refresher training that will be available where this will be required.
iii. Describe the supportive supervision that will be available to the implementation team.

5.4 Monitoring and Evaluation

This section is a guide to understanding the mHealth system's monitoring and evaluation (M&E) process. It highlights key elements that need to be in place to ensure the success of the M&E program. For mHealth systems to succeed, it is important to consider needs assessments, monitoring systems and outcomes evaluation that should be thoughtfully designed from the outset of systems formulation and implementation.

5.4.1 Monitoring and Evaluation of the mHealth System

To effectively monitor and evaluate mHealth interventions, it is imperative to use qualitative and quantitative research methodologies such as mHealth Evidence Reporting and Assessment (mERA) checklist. The mERA checklist seeks to standardize the reporting of mHealth findings and to promote the expansion of the evidence base by:

- Supplementing existing reporting standards to provide a concrete checklist of criteria specific to reporting on digital innovations; and
- Elaborating on the existing criteria to support high-quality methodological reporting of evidence.

M&E should be considered for the following processes:

i. Development and design of mHealth systems
ii. mHealth system planning and implementation processes, including key decisions and the rationale
iii. Documentation process
iv. Performance monitoring
v. Health impact monitoring and evaluation

The identification of the indicators that will be used to measure the success of the program shall be conducted using the following elements:

i. Usability: ease of use
ii. Integration
iii. Sustainability
iv. Scalability
v. Data quality, integrity and governance
vi. Service quality: improved service delivery
vii. Informative/educational information
viii. Rate of adoption; number of users

ix. Financial cost of implementation and analysis of cost-benefit ratio
x. Health benefits and health equity considerations

The following factors should be considered in any mHealth system M&E framework

i. Whether the system's M&E indicators meet the evidence and reporting requirements of MOH and other relevant stakeholders
ii. Whether the system showcases that MOH standardized health indicators have been incorporated into the M&E plan of the system
iii. Whether the data generated by mHealth platforms shall be used for evaluation and reporting
iv. Whether the proposed evaluation design is feasible and appropriate given the resources available
v. How the information and feedback generated by M&E will be incorporated into system design and implementation on an ongoing basis

5.4.2 M&E of the Implementation of mHealth Standards and Guidelines

Effective monitoring and evaluation of the implementation of the mHealth Standards and Guidelines shall adopt the following indicators:

i. Number of counties in which MOH has disseminated the standards and guidelines.
ii. Number of counties successfully implementing the standards and guidelines.
iii. Number of mHealth practitioners trained on the standards and guidelines.
iv. Number of mHealth practitioners accessing the standards and guidelines.
v. Number of mHealth practitioners who correctly understand the standards and guidelines.
vi. Number of stakeholders who adhere to the standards and guidelines.
vii. Number of mHealth systems that follow the required development steps.
viii. Number of mHealth practitioners who have implemented their systems by using the standards and guidelines.

5.5 Scaling Up

After piloting, the mHealth application in beta version should be scaled up. The scale-up should be based on addressing all the issues raised in the beta launch. The mHealth implementation should cater for scale-up by:

i. Considering sustainability and scalability of the system right from the beginning.
ii. Formulating a long-term plan for financing the mHealth systems project to ensure its sustainability beyond the beta (pilot) phase.
iii. Assessing the needs and demands of the target audience and being sure to understand local health priorities and the local technological, political, and programmatic landscape.
iv. Identifying existing similar mHealth efforts to avoid duplicating work that has already been done.

v. Educating and engaging end users and target beneficiaries throughout the mHealth system development process to foster acceptance.
vi. Ensuring that the mHealth system is aligned with local and national health priorities and that it is compatible with existing health information systems.
vii. Taking steps to foster buy-in from government, communities and local health systems from the beginning of the planning process.
viii. Working closely with local implementation partners to ensure that the content and format are user-friendly and accessible to target beneficiaries.
ix. Continually and systematically monitoring and evaluating mHealth systems to assess impact and identify necessary adjustments.
x. Ensuring that an mHealth system is not implemented using a silo approach and that it is open to be integrated with other mHealth systems.

In addition, mHealth implementers shall need to utilize well known frameworks such as the WHO mHealth Assessment and Planning for Scale (MAPS) toolkit to guide their scaling up process.

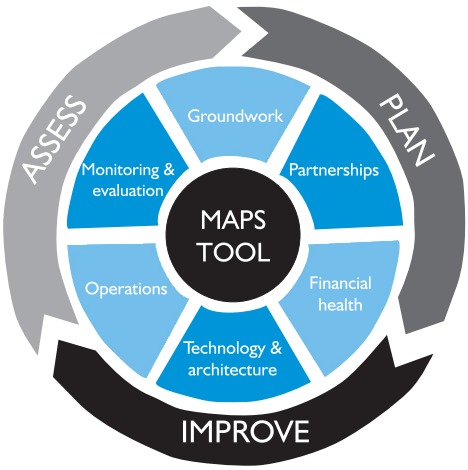


Figure 5.2: WHO's MAPs Framework

MAPS framework lays out six overarching thematic areas designed to provide actionable information for project teams to consider and address diverse concerns relating to scaling up and sustainability of mHealth deployments.

These six areas, also known as axes, are: Groundwork, Partnerships, Financial health, Technology and architecture, Operations, and Monitoring and evaluation

6. GOVERNANCE AND POLICY

6.1 mHealth Governance

Leadership and governance entails ensuring the strategic policy frameworks, such as national health strategies, plans and budgets, are in place and that these policy frameworks are combined with effective oversight, coalition-building, regulation, attention to system design and accountability. This involves competent direction of resources, performance, and stakeholder participation in ways that are open, transparent, accountable, equitable, and responsive to the needs of the people. Governance for mHealth embraces the principles described above and includes the components detailed below.

6.2 Governance Structure

mHealth is a component of the national health initiative addresses by the Kenya eHealth policy, Vision 20130, Health Policy and ICT Master Plan. It shall be managed within the established eHealth governance structure shown in Figure 6 as stipulated in Kenya's eHealth Policy 2016-2030).

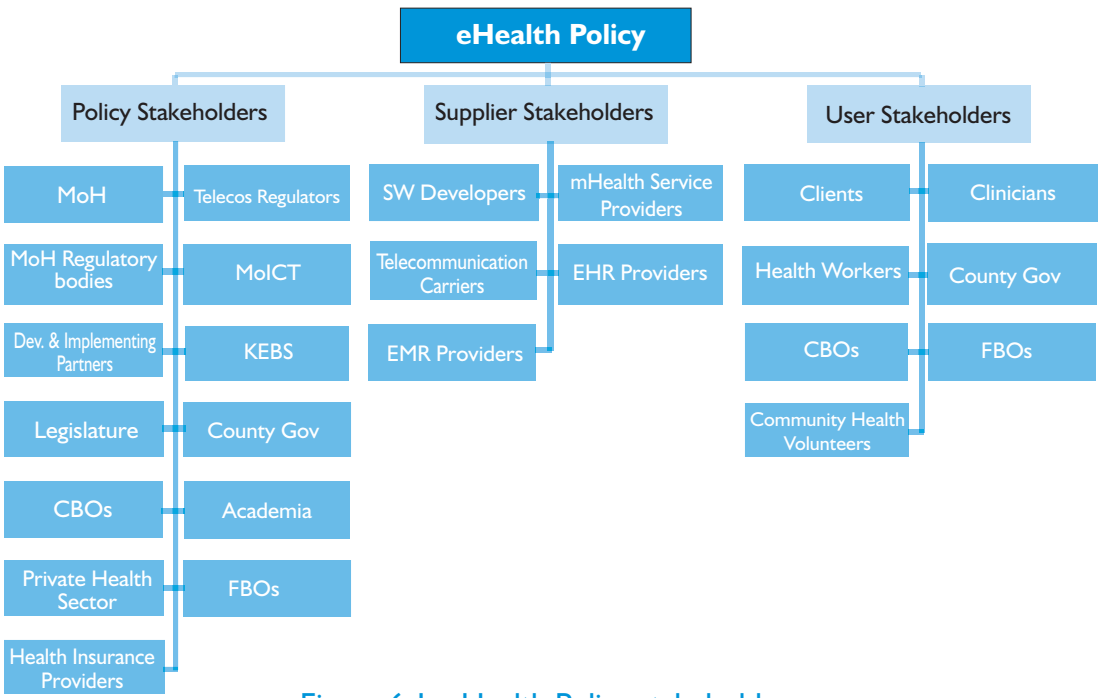


Figure 6.1: eHealth Policy stakeholders

6.3 Stakeholders

The stakeholders involved in the governance of mHealth systems can be classified into three broad categories, namely, policy stakeholders, implementing partners /suppliers, and users.

6.3.1 Policy Stakeholders

This category of stakeholders includes regulators, consultants and other interest groups, such as development partners, associations of clients etc. Specifically, these are:

i. Ministry of Health (MOH)
ii. Telecommunication regulators, such as the Communication Authority of Kenya (CA) and the ICT Authority (ICTA)
iii. Health regulatory bodies, including the Kenya Medical Practitioners and Dentists Board, the Pharmacy and Poisons Board, the Kenya Medical Laboratories Technicians and Technologist Board, the Clinical Officers Council, and the Nursing Council of Kenya, among others
iv. Ministry of Information and Communications Technology
v. Development and implementing partners
vi. Kenya Bureau of Standards (KEBS)
vii. Legislative bodies
viii. County governments
ix. Community- Based Organizations (CBOs)
x. Academia and research institutions
xi. Private health sector
xii. Faith-based Based Organizations
xiii. Health insurance providers

6.3.1.1 Roles and Responsibilities of Policy Stakeholders

Policy stakeholders shall have the following roles and responsibilities:

i. Formulating strategic policies and frameworks, such as national health policies, strategies, standards, plans and budgets
ii. Enforcement of standards and regulations
iii. Providing effective oversight
iv. Coalition-building and networking
v. Participating in the system design process
vi. Updating mHealth regulatory framework
vii. Allocating resources for the implementation of the standards and guidelines
viii. Performance monitoring
ix. Building county capacity for strategic leadership
x. Ensuring security of data
xi. Facilitating functioning of stakeholder coordination bodies

6.3.2 Supplier Stakeholders

This category of stakeholders includes mHealth device manufacturers and application developers, distributors and ecosystem providers who create an environment that enables the mHealth devices to be used. Specifically, this category includes:

i. Software (application) developers
ii. mHealth service providers
iii. Telecommunication carriers (companies)
iv. Electronic health record (EHR) providers
v. Electronic medical record (EMR) providers

6.3.2.1 Roles and Responsibilities of Supplier Stakeholders

The roles and responsibilities of the supplier stakeholders shall be:

- Ensuring that commodities and services are provided as per the requirements of this standard and guidelines
- Validating data to ensure that the data in the repository is useful
- Managing and resolving data related issues
- Putting mechanisms in place to reduce data security risks
- Participating in software development
- Validating the accuracy of the mHealth system
- Providing information required for access control management
- Deploying the mHealth systems

6.3.3 User Stakeholders

This category of stakeholders includes health service providers who deploy the mHealth applications for the benefit of their clients and also the clients themselves, who are considered the users of the mHealth applications. Specifically, this category will include:

i. Clients
ii. Clinicians
iii. Health workers
iv. County governments
v. Community-based Organizations
vi. Faith-based Organizations
vii. Community health volunteers

6.3.3.1 Roles and Responsibilities of Users

The following are the roles and responsibilities of users as stakeholders in mHealth systems:

- Implementing the mHealth applications
- Ensuring data security
- Ownership of the system
- Day-to-day administration of the system
- Adoption of mHealth systems
- mHealth resource management
- Monitoring and evaluation of the system

6.4 Regulatory Instruments

The mHealth Standards and Guidelines shall be anchored on the Health Policy, Health Bill 2015, eHealth Policy 2016-2030, Kenya eHealth Strategy 2016-2020, ICT Policy, and other government policies, which include the Kenya Constitution 2010 and Kenya Vision 2030.

6.5 Regulation

6.5.1 Certification Framework

In order to ensure that mHealth applications conform to the required standards, they shall be subjected to certification processes. The certification shall be based on the Kenya health information systems certification framework.

6.5.2 Protection of Privacy and Confidentiality

All the data collected using mHealth applications must be protected according to the laws governing protected health information and personally identifiable information.

6.5.3 Management of Disclosure of Health Information

Health information should be confidential. It should only be disclosed within the laid down procedures for sharing and disclosing health information, as described in sections 5 and 9 of these standards and guidelines, and in compliance with article 9 and 10 of the Health Bill 2016. Any instance of unauthorized disclosure must be reported immediately in accordance with laid down procedures.

People managing client data need to be sensitized on health data confidentiality and must sign non-disclosure agreements. For research purposes, the clients must provide informed consent by consenting and signing an ethically approved consent form before their data can be collected. All research work relating to client health information must be approved by the relevant ethics review boards (ERBs). The data must be stored as outlined in the research protocol, which must comply with security requirements, as outlined in section 2 of these standards and guidelines

6.5.4 Source Code and Application Ownership

Vendors or partners who build applications for the government shall hand over the source code to the MOH/county government, while applications developed in-house by government technical teams shall have their source code handed over to the relevant officer as a signing off requirement. All software developed for the government must be fully documented and should have the three classes of documentation as outlined in section 2.1 of these standards and guidelines.

6.6 Data Governance

6.6.1 Security

Governance of data in the mHealth system shall ensure that appropriate measures assuring data security have been put in place. This shall entail ensuring that data confidentiality, integrity, availability and non-repudiation of users are enforced for all client data as described in section 2.3.1 of these standards and guidelines.

6.6.2 Validation

The governance of data shall ensure that the quality of data held in the mHealth system is assured by enforcing measures of validation at collection points and in storage as described in section 2.3.5 of these standards and guidelines.

6.6.3 Accountability

Assurance processes shall be put in place to ensure that the accountability needs of the data are met. This can be achieved through user logs, audit trails, strong credentials based access, role based access to privileges, and quality assurance as described in section 2.3.1.4 of these standards and guidelines.

6.6.4 Ownership

Data collected from a client through use of mHealth applications shall be owned and held in trust by the government but the client shall have right of access to the data in order to facilitate further treatment and/or follow up. The records shall be retained where they are created, ensuring that reporting happens according to laid down procedures. In circumstances where the source data may be required by the government, such data should be availed and the appropriate laws and regulations governing the use, transmission and sharing of client data shall be observed at all times. In circumstances where the mHealth system is being handed over to the government after a period of operation, the data collected during that period of operation shall also be handed over. Communication context and content used in mHealth applications shall remain the property of the Government of Kenya and cannot be transferred without written approval from the relevant ministry, e.g. Ministry of Health.

7. LEGAL AND ETHICAL CONCERNS IN MHEALTH

The Kenya mHealth system standards and guidelines cover the legal and ethical concerns in the mHealth application development and implementation. These include the liability of the community health volunteer in the data transmitted from the mobile device he/she has, the fact that delivery of health services may involve the sharing of client data, shared confidentiality, transmission of the same data over wireless connections, and data encryption considerations.

The client health information stored offline on the mobile device should be protected from unauthorized access. The mobile application should have at least two levels of data access control to client information by health service personnel and should be based on their levels of health care provision. There should be access control mechanisms implemented and the ethical standing should prevail.

Developers of mHealth systems must take the necessary steps to apply the principles of domestic legislation, such as the Draft National Health Bill 2015, the Constitution of Kenya 2010 and the eHealth policy, in order to ensure that fundamental human rights of all individuals are respected with regard to processing of personal data. Implementers of mHealth system must ensure that:

i. Data is obtained and automatically processed fairly and lawfully.
ii. Data is collected for specified and legitimate purposes only.
iii. Data is not used in any way that is incompatible with the purposes for which it was collected.
iv. Data is stored only for as long as it is required for these purposes.
v. Data is recorded in an adequate, relevant, and non-excessive (proportional) manner visa-vis the said purposes.
vi. Data must be accurate.

Generally, mHealth systems must conform to ethical and legal requirements relating to:

i. Ownership of data and information.
ii. Access and disclosure of patient data.
iii. Usage of patient data.
iv. Storage of Personal Health Information and Personally Identifiable information.
v. Storage of health data: Health data must not be stored out of the jurisdiction of the Republic of Kenya without a written permission from the Ministry of Health (MOH).
vi. Remote diagnosis and prescription of medicine: The mHealth system must maintain confidentiality as per the eHealth policy guidelines.
vii. Technology: Collection, storage, transmission, sharing and usage of patient data must be within the confines of the legal framework embodied in the Kenya Health Bill 2015, the Constitution of Kenya 2010, the Records Disposal Act, HIE guidelines and Data Protection Act requirements.
viii. Any mHealth system must not infringe on any person's intellectual property rights.

The mHealth solution must also comply with the legal requirements stipulated in the following national policies and Acts of parliament:

- Kenya National Cyber Security Strategy
- Kenya Information Act 2013
- Data Protection Act
- Kenyan Archives Act
- KEMRI ethical guidelines

In principle, in order for mHealth systems to meet the legal and ethical requirements, it should also conform to the following WHO guidelines:

i. All PII information about a patient's health status, medical condition, diagnosis, prognosis and treatment and all other information of a personal kind must be kept confidential, even after death.

ii. Confidential information can only be disclosed if the patient gives explicit consent or if the law expressly provides for this. Consent may be presumed where disclosure is to other health care providers involved in that patient's treatment.

iii. All identifiable patient data must be protected. The protection of the data must be appropriate to the manner of their storage. Human substances from which identifiable data can be derived must be likewise protected.

iv. Patients have the right of access to their medical files and technical records and to any other files and records pertaining to their diagnosis, treatment and care and to receive a copy of their own files and records or parts thereof; such access excludes data concerning third parties.

v. Patients have the right to require the correction, completion, deletion, clarification and/or updating of personal and medical data concerning them which are inaccurate, incomplete, ambiguous or outdated, or which are not relevant to the purposes of diagnosis, treatment and care.

vi. There can be no intrusion into a patient's private and family life unless and only if, in addition to the patient consenting to it, it can be justified as necessary to the patient's diagnosis, treatment and care.

vii. Medical interventions may only be carried out when there is proper respect shown for the privacy of the individual. This means that a given intervention may be carried out only in the presence of those persons who are necessary for the intervention unless the patient consents or requests otherwise.

viii. Patients admitted to health care establishments have the right to expect physical facilities which ensure privacy, particularly when health care providers are offering them personal care or carrying out examinations and treatment.

8. COMPLIANCE

Compliance is the act or process of doing what is required of you, and in formal settings, includes providing evidence (documentation) of having adhered to the said requirements. The requirements could include laws, policies, regulations, guidelines, standards, methods or processes.

The mHealth standards and guidelines clearly define applicable requirements for proper implementation of mHealth systems, applications and interventions. Stakeholders involved in mHealth shall comply with these standards and guidelines in order to ensure best practice, and harmonization within the ecosystem. Compliance also improves monitoring and evaluation, interoperability, data sharing and service delivery in the health sector. Figure 8 below shows a compliance framework comprising of Commitment, Implementation, and Audit components.

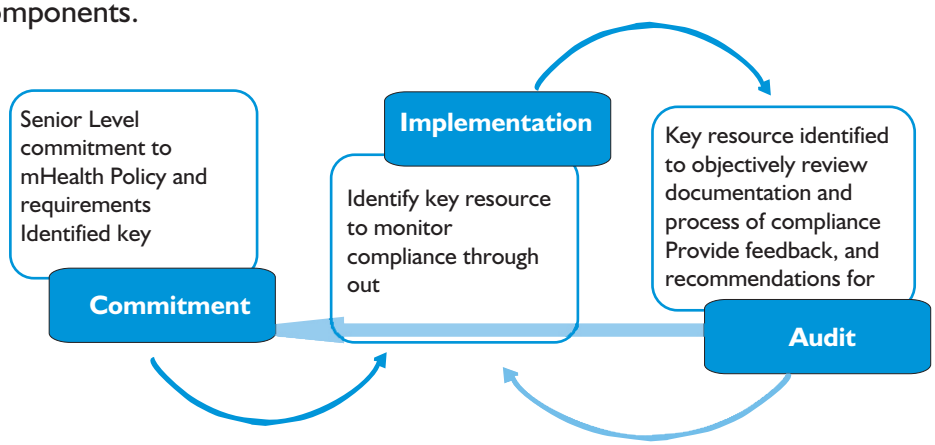


Figure 8:1: Compliance Framework

1. Commitment: Senior level commitment to complying with the mHealth Standards is required of stakeholders. This includes identifying an accountable resource (officer, manager) to ensure compliance to the standards.
2. Implementation: Stakeholders should identify a key resource within the organization to identify and monitor implementation of key requirements during the design, development, implementation and monitoring of mHealth systems. The assigned person should also responsible for documenting the level of compliance.
3. Audit: Stakeholders will also be required to identify a resource person to audit (confirm compliance) on behalf of management. This resource person will provide feedback and recommend corrective action for non-compliance. Upon compliance, the Audit resource person shall report to management on the level of compliance by all mHealth systems under implementation in Kenya.

Non-compliance with the mHealth standards and guidelines shall lead to fines, penalties and other consequences as spelt out in various laws governing both the health and ICT sectors.

ANNEXES

Annex 1: Sample M&E indicators that may be used in mHealth project

PROGRAM ELEMENTS	SAMPLE INDICATORS
Health outcomes	These tracks Changes in: • Contraceptive prevalence rate (CPR) • Maternal mortality rate • Rate of new HIV infection • Nutritional status (rates of anaemia, stunting etc)
Health behaviours	Tracking changes in: • Demand for health services related to mHealth program • Percent of women breastfeeding • Adherence to antiretroviral therapy • Contraceptive continuation
Acceptability of the program	• Percentage of subscribers retained • Percentage of users who unsubscribe • User-reported satisfaction
Quality and accessibility of mHealth services	• Number of regular mHealth program users • Profile of mHealth users (gender, age, location, economic and social status) • User-reported satisfaction • Messages to target audience delivered in a timely manner • Quality of data collected via mHealth application • Level of use of health services related to mHealth program • Percentage of messages vetted by technical experts
Health worker performance	• Change in volume of clients served • Client-reported satisfaction • Supervisor-reported performance observations
Capacity of the county and other levels of governance implementing organizations responsible for program and health	• Number and duration of program-related trainings in the county etc • Number, nature, and duration of successful partnerships
Program sustainability, program costs, and cost effectiveness	• Number and nature of funding sources • Total cost of ownership • Average cost of mHealth program per beneficiary • Money saved per beneficiary by change in target health behaviour or health outcome • Willingness of user to pay for mHealth services
Capacity of target beneficiaries	• Increased use of related health services • Demonstrated understanding of health concept(s) addressed by mHealth program • Change in target health behaviour
Extent to which the program operates in an enabling environment	• Existence of supportive policies and procedural guidelines • Adherence to interoperability standards and program procedures • Ongoing allocation of resources in budget for mHealth program • Action steps taken by program management team to enforce implementation-related changes

Annex 2: References and Bibliography

1. B. James, "Addressing the Need for Business Process Automation in Healthcare Claims," HealthCare Information Management, Inc. (HCIM), 17 03 2015.
2. J. Dias, "Big Benefits of Applying Automation to Healthcare," ed. 2014
3. M. Bergaus, "Presentation of Findings," in Design Issues for Service Delivery Platforms, Springer Vieweg , Berlin:2015, pp. 171-231.
4. M. Braunstein, Practitioner's Guide to Health Informatics, New York: Springer International Publishing, 2015.
5. R. Chejkova-Nikolov, M. Gusev, M. Kostoska and S. Ristov, "Interoperablity of bank statements: A case study", 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015.
6. The Government of Kenya, The Constitution of Kenya, Nairobi: National Council for Law Reporting with the Authority of the Attorney General, 2010.
7. N. Voros and C. Antonopoulos, Cyberphysical Systems for Epilepsy and Related Brain Disorders, 1st ed. Cham: Springer International Publishing, 2015.
8. The Government of Kenya, Data Protection Act 2012, Nairobi. Government Printer.
9. A. Dillon, "Chapter 381. Evaluation of Software Usability," in International Encyclopedia of Ergonomics and Human Factors, Second Edition - 3 Volume Set, Boca Laton, CRC Press, 2006.
10. HealthIT, Managing mobile devices in your healthcare organization, HealthIT.gov, 2017.
11. Finnell and B. Dixon, Clinical Informatics Study Guide, 1st ed. Cham: Springer International Publishing, 2016.
12. H. Leene, "A declaration on the promotion of patient' rights in Europe", Tijdschrift voor Gezondheidsrecht, vol. 18, no. 5, pp. 100-106, 1994.
13. M. Hardiman, T. Edwards, and C. PerfectServe, "Clarifying the confusion about HIPAA-compliant texting," ed, 2013.
14. A. Hauser and F. Roedler, "Interoperability: the key for smart water management", Water Science & Technology: Water Supply, vol. 15, no. 1, p. 207, 2015.
15. US Federal Government, “Learn more about Health Information Exchange (HIE) Benefits | Providers & Professionals | HealthIT.gov", Healthit.gov, 2017.
16. US federal Government,” Managing Mobile Devices in Your Health Care Organization”, HealthIT.gov, 2017.
17. US federal Government, “Take Steps to Protect and Secure Information When Using a Mobile Device", 2017.
18. Health Level Seven International,"HL7 Standards Product Brief - HL7 EHR-System Functional Model, R2", Hl7.org, 2007.

19. Health Level Seven International, "HL7 Standards Product Brief - HL7 Version 3 Standard: Privacy, Access and Security Services (PASS); Access Control, Release 1", Hl7.org, 2017.
20. Health Level Seven International, "HL7 Standards Product Brief - HL7 Version 3 Standard: Privacy, Access and Security Services; Security Labeling Service, Release 1 (SLS)", Hl7.org, 2017.
21. ISO, "ISO/TR 20514:2005 - Health informatics -- Electronic health record -- Definition, scope and context", Iso.org, 2005.
22. ISO, "ISO/IEC 27001 Information security management", Iso.org, 2013.
23. ISO & IEC, "Health informatics - Information security management in health using ISO/IEC 27002", Iso.org, 2013.
24. ISO, "ISO 18308:2011 - Health informatics -- Requirements for an electronic health record architecture", Iso.org, 2011.
25. ISO/TS, "ISO/TS 22220:2011 - Health informatics -- Identification of subjects of health care", Iso.org, 2011.
26. KEMRI, "Research Ethics", Kemri-wellcome.org, 2017
27. Ministry of Medical Services & Ministry of Public Health and Sanitation, Health Information System Policy, Nairobi: MMS.
28. The Government of Kenya, Kenya Information and Communications Act, Nairobi: National Council for Law Reporting. 2015
29. The Kenyan Government, The Kenya Information And Communications (Amendment) Act, 2013 (No. 41A of 2013), Nairobi: The Kenya Gazzette, 2013.
30. The Kenyan Government, The Health Bill 2016, Nairobi: Kenya Gazette Supplement No. 44 of 2015 , 2016
31. The Kenyan Governement, Public Archives and Documentation Service Act. Chapter 19. Revised Edition 2015 [2012], Nairobi: The National Council for Law Reporting, 2015. GSMA, MHealth and The EU regulatory Framework for Medical Services, London: Connected Living, 2014.
32. T. K. Government, The vision 2030, Nairobi, 2008.
33. Q. Tonig, W. Gao, Remote sensing and space technology for multidisciplinary research and applications, 1st ed. SPIE, 2006.
34. M. Eichelberg, T. Aden, J. Riesmeier, A. Dogac and G. Laleci, "A survey and analysis of Electronic Healthcare Record standards", ACM Computing Surveys, vol. 37, no. 4, pp. 277-315, 2005.
35. P. Mechael, "The Case for mHealth in Developing Countries", Innovations: Technology, Governance, Globalization, vol. 4, no. 1, pp. 103-118, 2009.
36. GSMA, MHealth and The EU regulatory Framework for Medical Services, London: Connected Living, 2014
37. WHO, "Launch of mHealth toolkit to help innovators scale up projects for reproductive, maternal, newborn, child and adolescent health", World Health Organization, 2017.

38. WHO, "New checklist published to help improve reporting of mHealth interventions", World Health Organization, 2017.
39. A. Mosa, I. Yoo and L. Sheets, "A Systematic Review of Healthcare Applications for Smartphones", BMC Medical Informatics and Decision Making, vol. 12, no. 1, 2012.
40. ICTA, Kenya National Cybersecurity Strategy 2014, Nairobi: Ministry of ICT, 2014.
41. Khealth, "Planning for Implementation | K4Health", K4health.org, 2017.
42. J Puustjärvi and L. Puustjärvi, "Ontology-based integration of clinical documents", Proceedings of the 14th International Conference on Information Integration and Web-based Applications & Services - IIWAS '12, 2012.
43. H. Have and B. Gordijn, Handbook of Global Bioethics, 1st ed. Dordrecht [u.a.]: Springer, 2014.
44. University of Denver, "Text Messaging in Healthcare Research Toolkit", Ucdenver.edu, 2017.
45. H. L. Wallace, "Electronic Publishing," in The Process of New Drug Discovery and Development, Second Edition, ed: Informa Healthcare, 2006, pp. 481-482.
46. L. Yoda, D. Nahl and M. Crosby, "Stage-Based mHealth Communication Interventions for HPV Education", 2013 46th Hawaii International Conference on System Sciences, 2013.

Annex 3A: List of Lead mHealth Experts

Name	Organization
1. Prof. David Ngaruiya	International Leadership University
2. Dr. Elisha Abade	University of Nairobi
3. Onesmus M. Kamau	MOH – Head eHealth Development Unit
4. Dr. Stephen N. Mburu, PhD	Modern Technology Computer Centre Ltd
5. Dr. Shem M. Angolo, PhD	Theo Computer Systems Ltd.
6. Dr. Cathy Mwangi	mHealth Kenya
7. Ms. Nancy W. Macharia	Samnet Communications Services Ltd
8. Prof. Peter Waiganjo Wagacha	University of Nairobi
9. Steven Wanyee	KEHIA
10. Willie Ngumi	GSMA
11. Dr. Abel Nyakiogora	Ministry of Health
12. Dr. Doris Kirigia	KEMRI Wellcome Trust
13. Dr. Geoffrey W. Chcemwa, PhD	JKUAT

Annex 3B: List of Review Committee

Name	Organization
1. Dr. David Soti	Ministry of Health
2. Ronald Osumba	Oracle
3. Dr. Peter Cherutich	Ministry of Health
4. Sophia Karanja	Ministry of Health
5. Gladys Echesa	Ministry of Health
6. Rachael Wanjiru	Ministry of Health
7. Nyokabi Njogu	Ministry of Health
8. Diane Kamar	Ministry of Health
9. Charles Mito	USAID MEASURE Evaluation PIMA
10. Joseph Mugah	USAID MEASURE Evaluation PIMA
11. Catherine Wanjiru	Samnet Communications Services Ltd

Annex 3C: List of Supporting Organizations

1. Ministry of Health
2. PEPFAR
3. USAID
4. CDC Kenya
5. KEMRI Wellcome Trust
6. IDRC
7. mHealth Kenya
8. USAID MEASURE Evaluation PIMA
9. WHO
10. AfyaInfo

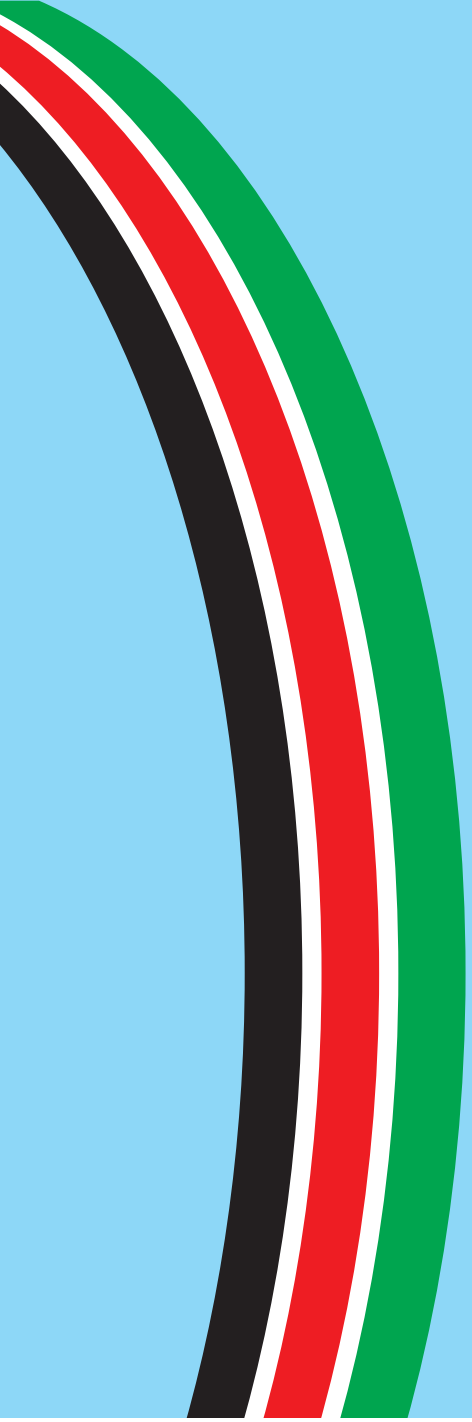
Annex 3D: List of Contributors

Name	Organization
1. Achieng Victor	Pathfinder International
2. Agnes Mana	Turkana County
3. Anne K. Barsigo	MOH - eHealth
4. Anne Koimur	Egerton University
5. Apollo Muchilwa	MOH - ICT
6. Asadhi Elijah	KEMRI
7. Ben Magoha	KEMSA
8. Benjamin Makau	Makueni County
9. Benson Karanja	Dimension Data
10. Bernard Ajwang	Intrahealth
11. Bernard M. Wambu	MOH - Child Health & Adolescence
12. Beryll Semmo	Kisumu County
13. Brian M. Mwaura	Savannah Informatics
14. Brian Omwenga	UON
15. Caroline Sang	MOH Community Health
16. Charles Kinuthia	MOH - HIS
17. Charles Mito	PIMA

Name	Organization
18. Chomba Ng'ang'a	Savannah Informatics
19. Christopher Ziroh	Kilifi County
20. Collin Sikwibele	Broad Reach Healthcare
21. Daniel Kiptum	AMPATH
22. Daniel Nanzai	MOH
23. David Kiminta	KMTC
24. Diana Mukami	AMREF - Health Africa
25. Diane Kamar	MOH - Community Health
26. Dorcas Nguyo	MOH - HIME
27. Dr. Abel Nyakiogora	MOH - Policy Planning
28. Dr. Beatrice Murage	Savannah Informatics
29. Dr. Cathy Mwangi	mHealth Kenya
30. Dr. Dan Orwa	UON
31. Dr. David Mbogori	KEMSA
32. Dr. David Soti	MOH - HIME
33. Dr. Doris Kirigia	KEMRI Wellcome Trust
34. Dr. Elisha Abade	UON
35. Dr. Elizabeth Ogaja	Kisumu County
36. Dr. Emmanuel Loiposha	Makueni County
37. Dr. G. K. Toromo	Baringo County
38. Dr. Gondi Joel	Migori County
39. Dr. H. Karamagih	WHO
40. Dr. Hillary Kipruto	WHO
41. Dr. Isabel Akinyi	Kisumu County
42. Dr. John Muthee	Savannah Informatics
43. Dr. Kabii Mungai	Nakuru County
44. Dr. Martin Osumba	AfyaInfo
45. Dr. Ngure Nyaga	Savannah Informatics
46. Dr. Njeri Mwaura	World Bank
47. Dr. Prachi Mehta	CDC Kenya
48. Dr. Salim Ali Hussein	MOH - Community Health
49. Dr. Sarah Chuchu	MOH

Name	Organization
50. Dr. Torooti Mwirigi	Care Pay
51. Dr. Shem M. Angolo, PhD	Theo Computer Systems Ltd.
52. Dr. Stephen N. Mburu, PhD	Modern Technology Computer Centre Ltd
53. Elijah Odhiambo	Migori County
54. Eunice Ndung'u	UNICEF
55. Everlyne Etemesi	MOH - KNBTS
56. Faith Muigai	Jacaranda Health
57. Festus Muema	Machakos County
58. Francis Thion'go	JKUAT
59. Gachoka Kiongo	KNH
60. Gladys Echesa	MOH - eHealth
61. Hezron Muriuki	mHealth Kenya
62. Imeraan Cassiem	Broad Reach Healthcare
63. Isaiah Nyabuto	MOH - eHealth
64. Isaya Opondo	Synergy
65. James Kwach	CDC Kenya
66. James Madiri	Migori County
67. Jonathan Ndede	mHealth Kenya
68. John Mwihia	MOH - NPHLS
69. Josca Korir	Treasury ICTA
70. Joseph Macharia	MOH - HIME
71. Joseph Ondigi	Broad Reach Healthcare
72. Joy Kiguta	Savannah Informatics
73. Justus Elung'at	AMPATH
74. Lilianna Assumpta	Egerton University
75. Macloud Ndua	Nakuru County
76. Mercy Tsimbiko	MOH - Community Health
77. Meshack Mbinda	AMREF
78. Michael Kagiri	UON
79. Michael Onyango	Kisumu County

Name	Organization
80. Mohamed Ismail	KEMRI
81. Mugah Joseph	USAID MEASURE Evaluation PIMA
82. Nancy Macharia	Samnet Communications Services Ltd
83. Naomi Shiyonga	MOH - IDSR
84. Nyokabi Njogu	MOH - ICT
85. Onesmus M. Kamau	MOH – Head eHealth Development Unit
86. Zachariah Kimwetich	Baringo County
87. Patrick Musyoki	Machakos County
88. Paul Karimi	ICTA
89. Paul Malusi	MOH - NPHLS
90. Paul Mutinda	Savannah Informatics
91. Perpetua Nyakundi	MOH
92. Peter Muya	AfyaInfo
93. Philip Bill Okaka	Pathfinder International
94. Philip Muchiri	CHAI
95. Prof. David Ngaruiya	International Leadership University
96. Prof. Peter W. Wagacha	UON
97. Rachael Wanjiru	MOH - ICT
98. Raphael Pundo	AfyaInfo
99. Regina Mutuku	Medic Mobile
100. Robert Wathondu	MOH - Research
101. Rose Kiriinya Kinyua	Emory University
102. Ruth Ngechu	MOH - Community Health
103. Samuel Kanga	I-TECH
104. Samuel Njoroge	MOH-Community Health
105. Sophia Karanja	MOH - eHealth
106. Stephen Konah	Pathfinder International
107. Steven Wanyee	KEHIA
108. Washington Anyango	Treasury ICTA



Ministry of Health

USAID
FROM THE AMERICAN PEOPLE

PEPFAR

MEASURE
Evaluation PIMA

CDC
Centers for Disease Control and Prevention

WHO

mHealth
KENYA
Public Private Partnerships
We Develop, Implement & Sustain

KEMRI | Wellcome Trust

IDRC | CRDI
Canada

AfyaInfo
Kenya National HMIS Program