MINISTRY OF HEALTH

# Kenya Standards and Guidelines for E-Health Systems Interoperability

Version 2: July 2015

**July 2015**

**Recommended Citation:** Government of Kenya, 2015, Kenya Standards and Guidelines for E-Health Systems Interoperability, Nairobi, Kenya: Ministry of Health.

AfyaInfo is a technical assistance program to support the Government of Kenya to strengthen their health information systems. The program is implemented by Abt Associates, Inc. in partnership with Training Resources Group, ICF International, and the University of Nairobi. It is funded by the United States Agency for International Development (USAID), under the AIDS Support and Technical Assistance Resources (AIDSTAR) Sector II IQC, contract number GHH-I-00-07-00064-00 AID-623-TO-11-00005, Kenya Health Information System.

DISCLAIMER:

The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

# Table of Contents

## Foreword

The Ministry of Health recognises the important role played by appropriate application of relevant standards; guidelines and policy formulations to guide the health sector fulfil its mandate. In this regard the development of the just completed system interoperability standards and guidelines for electronic health systems could not have come at a better time than now. This is especially important as a means of enhancing efficiency and effectiveness in the delivery of health services in this country. Information systems interoperability standards and guidelines have the potential to impact upon almost every aspect within the health sector. In the public health, system interoperability standards and guidelines for information management and communication processes are pivotal in ensuring that all the systems are harmoniously sharing relevant data and discourages proliferation of information silos and parallelism of data collection systems in line with best national and global practices. Implementation and enforcement of these standards will go a long way in reducing duplication of efforts; promote data and information sharing among systems and harness appropriate use of ICT resources as an enabler to effectiveness and efficiency in delivery of health care services.

As the Ministry of Health (MOH) increasingly embraces the use of ICT in its service delivery, it is becoming more important to take a common approach based on recognised best practices. The Ministry recognises the need for a consistent approach to the development of ICT systems and, thus, the need to formulate these Standards and Guidelines.

The standards, guidelines and principles set out in this document shall be applicable to the health sector in all tiers of health care and health management both at National and County levels to support service delivery and to facilitate referral mechanisms. This document provides the much needed guidance towards establishing, acquiring and maintaining current and future 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 and development partners. Valuable input was received from a vast array of subject experts in different fields and interests. It referenced internationally recognised standards, best practices and principles and will be implemented in accordance with the existing Health Policy, ICT Standards, system interoperability principles and the Health Information Policy.

Lastly, it is my sincere hope that all the actors in health sector will rally behind these standards to ensure that we all steer the country towards the use of acceptable standards.

**Dr Nicholas Muraguri**
**Director of Medical Services**

## Acknowledgements

The realisation of these e-health Systems Interoperability Standards and Guidelines has been achieved through tremendous efforts and commitment of various individuals and organisations, from the initial draft through to the review.

We would like to acknowledge the contributions of Mr. James Macharia, Cabinet Secretary, and the Ministry of Health, whose leadership ensured that the document was realised.

Special thanks go to our Principal Secretary, Dr. Khadijah Kassachoon, whose enormous support and guidance led to the finalisation of the document.

Dr. Nicholas Muraguri, Director of Medical Services, ensured that there was full participation of Ministry staff and stakeholders in the entire process. Also critical from the inception to the finalisation of these Standards and Guidelines were the personal support and contributions of Dr. David Soti, Head, Division of Monitoring &Evaluation, and Health Informatics, Research Development

The process received tremendous financial and technical support from USAID through the AfyaInfo Project. Additional technical support was provided by CDC through ITECH Kenya. Many thanks to Dr Martin Osumba, Raphael Pundo, David Muturi, Solomon Simba, Erastus Mburu of AfyaInfo, and George Owiso, Sam Kanga of ITECH Kenya.

Special thanks go to Onesmus Kamau, Head E-health Unit, Anne Barsigo and other staff members from the HIME division; Dr. Martha Muthami, Head HIS unit, Francis Gikunda, Jeremiah Mumo, Nancy Amayo, Ann Gitungo, Esther Kathini, Margaret Chiseka, Robert Wathondu, Margaret Omondi, Abdullahi Kimogol, and Gladys Echesa. We also like to appreciate the support given to us by the Division support team who include Dorcas Nguyo, Joseph Macharia, and Aurelia for their contributions to the entire process of the development of this document.

Thanks are also goes to the Division of ICT staff members James Njiru, Rachael Wanjiru and Nicholas Ngari for their steadfast contribution to the realisation of this important document.

Since we may not be able to mention everyone by name, we wish to sincerely thank everyone who in one way or another participated in the development of these ICT System Interoperability Standards and Guidelines – including all the heads of departments and divisions, members of staff, and health sector stakeholders.

## The Document Development Process

The need for systems interoperability standards became apparent in the Health Information Systems Assessment Report[1] which identified lack of standardised and weak interoperability features in the development information systems in the health sector. The MOH quickly followed up this recommendation and through the Divisions of Heath Information Systems, Standards, and ICT and with support of USAID through the AfyaInfo Project conceptualized and produced the first draft of the Kenya e-Health Information Systems Interoperability Standards.

The draft was subjected to a wider stakeholder involvement through systematic review process that greatly enriched the content. The review team comprised of a select team of experts from Government Ministries of Health, Information and Communications Technology, the National Treasury, the academia, development and implementing partners and the private sector.

This team provided excellent input and ideas via several forums composed of a workshop and review meetings that produced this first edition of the interoperability standards.

[1] Government of Kenya. 2013. E-health Systems Assessment Report. Nairobi, Kenya: Ministry of Health, AfyaInfo Project.

## Authority

This documents development adheres to the Kenya National eHealth strategy 2011-2017, Vision and Mission (Ministries of Health, April, 2011) as well as the following;

1. Kenya Constitution 2010
2. Data Protection Act 1998/2003
3. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules
4. HIPAA 1999/2000/2001/2002
5. Health Records (Privacy and Access) Act 1997
6. 6 HIS Policy (2013-2030)
7. Kenya Health Policy Framework (2012-2030)
8. Health Sector ICT Standards and Guidelines (2013)
9. Government of Kenya. 2013. E-health Systems Assessment Report. Nairobi, Kenya: Ministry of Health, AfyaInfo Project.

## List of Acronyms

| | |
|---|---|
| ADT | Admission, Discharge and Transfer |
| CCR | Continuity of Care Record |
| DICOM | Digital Imaging and Communications in Medicine |
| EHR | Electronic Health Records |
| FHIR | Fast Healthcare Interoperability Resources |
| HIPAA | Health Information Portability and Accountability Act |
| HIS | Health Information Systems |
| HL7 | Health Level 7 |
| HL7 CDA | Health Level 7 Clinical Document Architecture |
| HL7 CCD | Health Level 7 Continuation of Care Document |
| HL7 DS | Health Level 7 Discharge Summary |
| ICD-10 | International Classification of Diseases -10 |
| ICT | Information and Communication Technologies |
| ISO | International Organization for Standardization |
| JSON | JavaScript Object Notation |
| KEMRI | Kenya Medical Research Institute |
| KEMSA | Kenya Medical Supplies Agency |
| LOINC | Logical Observation Identifiers Names and Codes |
| MEDS | Mission for Essential Drugs |
| MoH | Ministry of Health |
| NHIF | National Health Insurance Fund |
| NHIS | National Health Information System |
| PACS | Picture archiving and communication system |
| PEPFAR | President's Emergency Plan for AIDS Relief |
| R-ADT | Registration-Admission, Discharge, Transfer |
| SDMX | Statistical Data and Metadata Exchange |
| SDMX-HD | Statistical Data and Metadata Exchange- Health Domain |
| SI | International System of Units |
| SNOMED | Systematized Nomenclature of Medicine |
| SOAP | Simple Object Access Protocol |
| UML | Unified Modelling Language |
| USAID | U.S. Agency for International Development |

# Introduction

**Vision the e-health data exchange standards supporting the Kenya national e-health strategy. This is for developing efficient, accessible, equitable, secure and common fondly healthcare services inbound by IT.**

# 1.0 Data Exchange Standards

In order to support the interoperability between various data systems in the health sector, Health Information Systems should follow international data exchange standards, which include:

I) Clinical Terminology Standards: Systematized Nomenclature of Medicine (SNOMED) for point of care clinical work, International Classification of Diseases-10 (ICD-10) for administrative aggregate data, Logical Observation Identifiers Names and Codes (LOINC) for laboratories, RxNorm for pharmacies; and the current specified implementation guidelines for each of these. (RXNorm is a normalized naming system for generic and branded drugs, and a tool for supporting semantic interoperation between drug terminologies and pharmacy knowledge base systems.)

II) Clinical Messaging Standards: Health Level 7 (HL7)V 2.0 and above standards– e.g. Fast Healthcare Interoperability Resources (FHIR), and Digital Imaging and Communications in Medicine (DICOM)/picture archiving and communication system (PACS) for imaging; and their respective current implementation guidelines.

III) Administrative and Document Standards: The standards will indicate the type of information included in the document and the location of the information. Examples of document standards include the paper-based subject objective assessment protocol (SOAP) standard, and the HL7 derived standards –e.g., Clinical Document Architecture (Health Level 7 Clinical Document Architecture, abbreviated HL7 CDA) for electronic sharing of documents, the Continuation of Care Document (Health Level 7 Continuation of Care Document, abbreviated HL7 CCD), and the Discharge Summary (Health Level 7 Discharge Summary, abbreviated HL7 DS) – along with the current implementation guides for these standards.

## 1.1 Methods of Exchange

System owners may implement manual and automated methods of data exchange for their systems, but the latter method is preferred for data exchange between systems within the health sector.

**a. Manual**

This can be defined as data exchange that involves human steps or intervention. System owners who implement manual modes of transferring data between systems shall provide domain-specific data exchange templates.

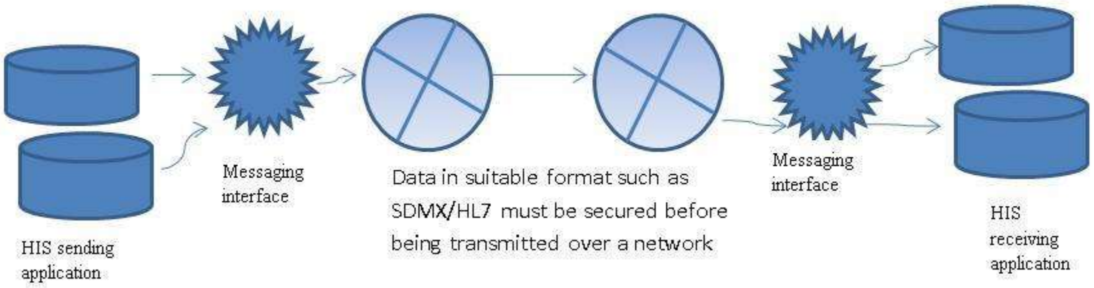
These system owners are responsible for ensuring sufficient levels of documentation to enable the exchange of data between different systems.

**b. Automated**

This can be defined as data exchange processes that involve minimal human interaction. This includes Application Programming Interface, agents, and "middleware." System owners shall be responsible for implementing an automated messaging interface for their systems. However, all systems with an automated data exchange format shall share data in Extensible Markup Language format, JavaScript Object Notation (JSON), or any other widely accepted standard.

The diagram below shows the generic function of a messaging interface between two electronic Information systems.

**Figure 1: Messaging Interface**


Messaging interface
Data in suitable format such as SDMX/HL7 must be secured before being transmitted over a network
Messaging interface
HIS sending application
HIS receiving application

## 1.2 Data Types and Units of Measure

The data types within the health information systems are usually derived from data elements in the following areas: clinical, human resources, logistics, and financial data. The data types should follow established and standard domain-specific units of measures as per International System of Units (SI) units or ISO (International Organization for Standardization) standards where applicable.

Examples of measures for common data types in the clinical domain include:

Table 1: SI Base Quantities and Units

| Metric Measure (Unit) | Base (Quantities |
|---|---|
| Centimeters (Cms) | Height |
| Kilograms | Weight |
| Degree Celsius | Temperature |
| Mm/hg | Blood pressure |
| Mmol/l | Blood sugar |
| A,AB,O,B<br>Can be either + or - | Blood group |
| Centimeters | Mid-upper arm circumference |
| dd/mm/yyyy | Dates e.g. date of birth |

## 1.3 Unique Identifiers

Identifiers are variables that uniquely distinguish people or entities within a specific domain. Health domain identifiers include:

**a. Patient Identifiers**

In the absence of the National Unique Patient Identifier, the following optional details may be included.

I. National Health Insurance Fund (NHIF)

II. National Social Security Fund (NSSF)

III. National Identity Number

IV. Passport Number

To uniquely identify a patient, the following attributes are mandatory when transmitting patient-level data.

I. National unique patient identifier (if available)

II. Patient names in full – At least three names

III. Gender

IV. Date of birth

In the absence of the National Unique Patient Identifier, the following optional details may be included.

I. National Health Insurance Fund (NHIF)

II. National Social Security Fund (NSSF)

III. National Identity Number

IV. Passport Number

**b. Facility Identifiers**

These shall be used to uniquely identify a facility providing a specific set of services. Facility identifiers shall include:

I. Master Facility List Code

II. Master Facility List Facility Name

III. Geocodes

**c. Health Care Professionals Identifiers**

Identification of health care professionals is important during creation of a patient-to-service provider relationship within a facility or during patient referral. The identifiers are also important when conducting human resource-oriented tasks. Identifiers for service providers – health care professionals whose practice is regulated by the Ministry of Health (MoH) and its regulatory bodies and agencies – during data exchange shall include:

I. Professional Registration Certificate number

II. National ID/Passport No.

III. Area of specialization

**d. Non-Medical Institutions Identifiers:**

These are organizations and corporate institutions that offer services and products within the Kenyan health sector; they include:

I. Identifiers for Private Medical Insurers as licensed by the Insurance Regulatory Authorities

II. NHIF

III. Any other officially recognized entity in the health sector

Identifiers for these groups will include but not be limited to registration number.

## 1.4 Administrative Levels of Data Exchange

Data exchange between systems in the health sector domain may happen at different levels. It is the responsibility of system owners to ensure that business process interoperability is achieved by ensuring that data moving across the various levels of exchange adhere to established business rules governing these processes. The guidelines governing these business rules will be provided where applicable by the MoH e.g., CCD implementation guidelines and templates.

### a. Community to Facility

Systems at this level exchange the following data:

I. Referrals, e.g., a Community Health Worker/Community Health Extension Worker doing a referral via mobile phone to a facility

II. Commodities and supplies

III. Demographic data

IV. Epidemiological data

### b. Within a Facility

The systems within a health facility exchange or share the following data:

I. Order entries, requests and results transmission – these include: Admission, Discharge and Transfer (ADT) orders, laboratory orders, imaging prescription orders, procedure orders, and commodities and supplies

II. Patient movements and locations between the wards and other departments

III. Between clinical systems, billing and claiming systems

### c. Facility to Facility

Systems in different facilities can exchange different types of data between themselves. These include patient and administrative data such as:

I. Referrals, patient summaries and reports in the standardized MoH format as defined in the Kenya Health Sector Referral Implementation Guidelines 2014. Any referral/patient summary message must be encoded in a HL7 document standard format, e.g. Continuation of Care Record on patient referral.

II. Order entries, requests and results transmissions, e.g. laboratory, imaging, prescription, procedures

III. Commodities and supplies

IV. Electronic consultations

### d. Facility to Other Entities

This data exchange scenario refers to the exchange of administrative data that is shareable between facilities and other independent entities e.g., research institutes (KEMRI and others), insurers (NHIF and other private insurers), commodities suppliers (KEMSA, MEDS and others), and development partners (USAID, PEPFAR, CDC, World-bank, UN and others).

### e. Facility to County

This data exchange refers to health and administrative data that is sharable between systems at the facility level and those at the county level. These systems exchange the following aggregate data:

I. Service delivery data

II. Public Health Surveillance data

III. Commodities and supplies data

IV. Electronic consultation

V. Financial data

VI. Human Resource data

**f. County to County**

This data exchange refers to administrative data that is sharable between systems of different counties. These systems exchange the following data:

I. Service delivery data

II. Public Health surveillance data

III. Commodities and supplies data

IV. Electronic consultation

V. Financial data

VI. Human Resource data

VII. Others as identified by the facility

**g. County to National**

County-level systems shall exchange specific data with systems at the national level. These data include:

I. Public Health surveillance data

II. Data on commodities and supplies

III. Service delivery data

IV. Electronic consultations

V. Financial data

VI. Human Resource data

# 2.0 Introduction

The exchange of data between health information systems requires high security standards to safeguard the data's integrity and confidentiality. The data exchanged may be patient-centric, administrative or aggregated, but irrespective of that it must be safeguarded

## 2.1 Information Security Standards and Guidelines

The exchange of data between health information systems requires high security standards to safeguard the data's integrity and confidentiality. The data exchanged may be patient-centric, administrative or aggregated, but irrespective of that it must be safeguarded.

This sensitive data should be protected by policies, rules and regulations to safeguard it from losses, unauthorized access, alterations and misuse. Whether the data is transmitted manually or electronically, health information systems must have clear standards and policies that guide how data is captured, accessed, stored, modified, transmitted, backed up and archived.

Ensuring the privacy and security of electronic health information is a key component to building the trust required to realize the potential benefits of electronic health information exchange. If individuals and other participants in a network lack trust in electronic exchange of information, due to perceived or actual risks to individually identifiable health information or to lack of confidence in the accuracy and completeness of such information, it may affect their willingness to disclose necessary health information, and that could have life-threatening consequences.

Privacy and Security Rules protect the privacy and security of individually identifiable health information.

## 2.2 Risk Management

This involves establishing, documenting and maintaining an ongoing process for identifying clinical hazards associated with a health software product, throughout the product's development lifecycle; estimating and evaluating the associated clinical risks; controlling these risks; and monitoring the effectiveness of the controls throughout the lifecycle. At the highest level, risk management requires:

- a complete understanding of the product/system
- appropriate awareness of the need for risk management
- the ability to identify relevant targets at risk
- a fully defined risk assessment process
- risk assessment to be carried out completely and competently
- appropriate lifecycle management to be in place

This process should include the following elements:

- identification  of context, requirements and scope
- creation of clinical risk management plan
- setting the requirements for and defining the competencies of personnel
- clinical hazard identification
- clinical risk analysis
- clinical risk evaluation
- clinical risk control
- creation of clinical safety case report(s)
- post-deployment monitoring
- post-production maintenance of the clinical risk management process

## 2.3 Security rules to govern data exchange

### 2.3.1 Administrative safeguards

These safeguards aim at protecting the confidentiality, availability, accountability and integrity of the data. They establish standards and specifications for health information systems security that include the following:

- Security management processes to identify and analyze risks to data and implement security measures to reduce risks
- Defined communication channels to manage the data exchange and the levels of authorization required
- Staff awareness and training to ensure knowledge of and compliance with the policies and procedures in place
- Information access management to limit access to Electronic Health Records (EHRs) in order to protect health information, including the information in Electronic Medical Records
- Contingency and business continuity plans to respond to emergencies or restore lost data

Health workers who have privileged access to a patient's records shall be accountable to maintain the highest level of confidentiality and ensure that sharing of data is practiced in the interest of the patient only.

Persons or entities implementing health information systems must ensure adherence to the Ministry of Health HIS policies and other government standards that guide the management of manual and digital documents.

All implementers and developers of health information systems should adhere to health sector Information and Communication Technologies (ICT) standards and guidelines on security in the management of data, server rooms, and information system components.

### 2.3.2 Physical safeguards

The developers, users, implementers and owners of health information systems should reference the Health Sector ICT Standards and Guidelines 2013. These standards include specific safeguards to control physical access to the data center. Some of the physical safeguards are:

- Installation of facility access controls, such as locks, closed-circuit television and alarms, to ensure only authorized personnel have access to facilities that house systems and data.
- Ensuring that workstation security measures are in place, such as cable locks and computer monitor privacy filters, to guard against theft and restrict access to authorized users only.
- Implementation of workstation use policies to ensure proper access to and use of workstations.

### 2.3.3 Technical safeguards

The developers, users, implementers and owners of health information systems should reference the Health Sector ICT standards and guidelines 2013. These safeguards include hardware, software, and other technology that limits access to electronic information.

Some of the required technical safeguards to be adhered to by all users, implementers and developers are:

- Access controls, so that only authorized personnel have access to the system
- Audit controls, to monitor activity on an electronic health information system
- Integrity controls, to prevent improper alteration or destruction of data
- Transmission security measures, to protect data when it is transmitted over an electronic network

## 2.4 Health Information Privacy

The 1998 Kenya Data Protection Act envisages complete transparency: to the extent possible, individuals should have a clear, unambiguous understanding of the purposes for which the data is collected and how it will be used. The Act also stipulates that when the data is being collected, individuals from whom the data is collected must give their informed consent, and have the opportunity to opt out of any later data rounds of data collection.

In the U.S., the Health Information Portability and Accountability Act (HIPAA) privacy rule on protected medical information ensures that the privacy of individuals' medical records and other personal health information is maintained. This rule also proposes civil and criminal penalties for any violations within the U.S. jurisdiction.

The draft Kenya Health Bill envisages that violations of stipulations regarding the protection of privacy and confidentiality of patient data will attract specific fines and other civil punishments. The draft Kenya Data Protection Bill covers the rules governing: the processing of personal data, protection and security of personal information, access to this data, and leeway for correction of information within the data by the affected subjects. Section 11 of the Data Protection Bill indicates that any agency storing personal data should put in place security safeguards that are reasonable in the circumstances to protect the data against loss, damage and destruction, and to protect the data from unauthorized persons' access, from modification, and from negligent disclosure or use. Sections 12 and 13 of the Data Protection Bill stipulate that any agency keeping personal data should enable the individual data subjects to obtain their data or confirm its presence while enabling its correction.

The tenets of HIPAA that have been borrowed and used as part of these e-Health interoperability standards are:

- In general, one may use or disclose protected health information for treatment, payment, and health care operations without obtaining a patient's written permission. For other purposes, such as marketing, one may need to obtain an individual's authorization to use or disclose the patient's protected health information.
- Any agreements involving sharing of personal health information must explicitly require those sharing it to comply with stated regulations, including breach notification requirements.
- Generally, anyone involved in data and information sharing must limit their access to, use of, and disclosure of protected health information to the minimum necessary to carry out an action. This is called the "minimum necessary rule." There are several exceptions to this rule. For example, one does not have to limit the disclosure of protected health information to the minimum amount necessary when disclosing the information for treatment of the individual.

# 3.0 System Interoperability Governance

Information governance consists of the processes, functions, standards and technologies that enable high-quality information to be created, stored, communicated, valued and used effectively and securely. The five tenets that ensure this is achieved are:

- **Data confidentiality:** requires policies, processes and solutions that prevent the unauthorized collection, storage, use and dissemination of information, by enforcing access restrictions and permissions defined by patients through consent-based access control models.
- **Data integrity:** refers to the validity, accuracy and reliability of data while it is being stored, transferred, retrieved or processed. It requires that data retain its meaning and clinical or administrative value after it has been communicated or used.
- **Data privacy:** requires policies and processes that enable patients to authorize and restrict access to identifiable data in e-Health systems. Data privacy requires sophisticated, consent-based access control models and permission regimes.
- **Data quality:** requires organizations to implement solutions with intelligent data handling and data management functionality that identify data errors and poor-quality data. Organizations can also improve data quality by enabling subsystems to share information more effectively through standardized data architectures and interfaces.
- **Data security:** requires organizations to develop security architectures that proactively manage security risks, effectively identify and prioritize threats, and rapidly address vulnerabilities.

### Table 2: Discipline and Component of System Interoperability Governance

| Stakeholder Cluster | Needs and Interests |
|---|---|
| Data confidentiality | Role-based access control models |
| | Patient and provider record sealing |
| | Identification and authentication |
| | Anonymisation and pseudonymisation |
| Data integrity | Code integrity |
| | System hardening |
| | Interoperability (organisational/process, semantic, syntactic and technical) |
| Data privacy | Patient consent models and mechanisms |
| | Patient-provider relationship-based access controls |
| | Patient access controls |
| | Effective data security and data handling policies |
| Data quality | Error correction |
| | Data validation |
| | System and interface certification |
| | Standards-driven architecture |
| Data security | Message integrity and communications security |
| | Event audit and alerting |
| | IT security audit |
| | Network integrity |
| Compliance and assurance | Audit governance , policies and standards |
| Availability | Business Continuity Planning<br>Disaster Recovery |

## 3.1 System Data Quality

Implementation of the data quality protocols will ensure that the processes around collecting, collating, analyzing, interpreting, disseminating, and using data meet data quality standards.

The system data quality assurance process will include:

Standardized data elements across health information systems participating in the National Health Information System (NHIS) published Metadata dictionary.

Adherence to a repository of validation rules that enforce business processes and comprehensive data cleaning procedures among system owners and implementers. (There is a need to build a repository of validation rules that govern how all the data elements being collected within the NHIS are processed and flagged for error, and also to build in robust data cleaning procedures.)

Development and enforcement of automatic tools that use business rules to reference data in order to analyze and rank it according to completeness, conformity, consistency, duplication, integrity and accuracy.

## 3.2 Operating Resources for Parties Exchanging Data

This refers to the reliability and availability of the components that collect, store and transmit data for purposes of interoperability. The parties involved should adhere to these guidelines for the purpose of seamless data exchange. These components can be broadly categorized into the following:

### 3.2.1 Hardware

This refers to all digital-enabled medical equipment and other ICT equipment that is used in service provision and in the process of collecting, storing and transmitting health-based data. This equipment should guarantee performance levels as per the guidelines below.

a. **Reliable hardware as per health sector ICT standards**

b. **Hardware that meets specific system requirements for systems participating in NHIS.**

c. **Guaranteed manufacturer support**

d. **Reference to Ministry of Health Data Centre guidelines**

### 3.2.2 Human Resources

This refers to the capacity and ability of people involved in the data exchange process. The human resources capacities and skillsets involved in data exchange should meet Data Centre guidelines and Ministry of Health ICT standards. Skilled staff will be needed across all domains, and must uphold professional standards and ethics.

### 3.2.3 Software

This refers to the intangible technological resources that run in the medical equipment and computing devices involved in collecting, managing and transmitting data. The standards for the software involved in the data exchange process should follow the guidelines below:

a. Data Centre guidelines enshrining standard software engineering metrics

b. Security standards as per health sector ICT standards

c. Guaranteed support

### 3.2.4 Connectivity

This refers to the media and devices that provide an end-to-end link for data exchange to occur.

a. Internet connectivity to servers available at 99.9%

b. Communication security standards as per health sector ICT standards

c. Guaranteed manufacturer support for the networking equipment

## 3.3 Summary/tabular representation of e-health Standards

All e-Health standards that will be applied can be broadly classified or grouped into the following categories:

- Identifier standards
- Messaging standards
- Coding and terminology standards
- Content and structure standards
- Electronic Health Record standards
- General IT standards
- Security standards

Table 3: Appropriate e-Health Standards Framework

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| | | **Identifier Standards** | |
| 1. | ASTM E1714 - 07 | Standard guide for properties of a universal health care identifier | The purpose of this standard is to ensure uniformity in the identification of patients in face-to-face encounters and computer-to-computer communication, and in the recording and reporting of patient identification data. The standard also ensures that the correct information is linked to the correct patient. It specifies |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| | | | the structure and data elements required for positive identification of patients in both face-to-face and computer technology-supported environments. It defines the demographic and other identifying data elements that should be captured, and provides guidance on their implementation in paper-based and computerised environments. |
| 2. | ISO/TS 27527:2010 | Provider identifier standard | This standard provides guidelines for the creation of unique identifiers for individual health care providers as well as the health care institutions where the care is provided. It specifies the data elements required to support both manual and automated identification of providers and health care institutions. |
| **Messaging Standards** | | | |
| 3. | DICOM | Digital Imaging and Communication in Medicine | Specifications for information object definitions, data structures and their semantics, protocols for the exchange of medical information among imaging equipment and other health care applications, file format and storage of medical images. DICOM has been adopted as an international standard for medical images by ISO under the title ISO 12052:2006. |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| 4. | HL7 | Health Level 7 | Enable the interchange of clinical and administrative data among heterogeneous health care applications in the form of patient demographics, health insurance data, clinical observations, appointment schedules and patient referrals. Unlike other health care messaging standards, which focus on specific health care domain (e.g., the exchange of laboratory results), HL7 messaging standards support the exchange of different types of health care data. |
| 5. | ISO 13606-5:2010 | Electronic Health Record Communication (part 5): Interface Specification | An EHR communication standard that specifies the information architecture required to support meaningful communications between systems and services that need or provide EHR data. It defines the Computational Viewpoint for different interfaces, without specifying or restricting their implementation approaches as messages or service interfaces. |
| 6. | ISO/HL7 27931:2009 | Data Exchange | This standard provides an application protocol for the electronic exchange of data in health care environments. |
| 7. | ISO/HL7 27951:2009 | Common Terminology Services | Framework for the development of an application programming interface that can be used by messaging software when accessing terminological content. It is not intended to be a complete terminology service in and of itself. |
| 8 | SDMX-HD | Statistical Data and Metadata Exchange – Health Domain | SDMX-HD is a statistical and metadata exchange-based standard adapted by WHO for the exchange of health indicator definitions, as well as data in aggregate data systems (e.g., DHIS). It specifies the structure and format of aggregate data for health indicator messages that are exchanged between HIS and monitoring and evaluation systems like the DHIS. |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| | | **Electronic Health Record Standards** | |
| 9. | ASTM E1239 – 04: 2010 | Standard Practice for Description of Reservation/Registration-Admission, Discharge, Transfer (R-ADT) Systems for Electronic Health Record (EHR) Systems | Definition of the minimum information capabilities of R-ADT system. It describes the processes of patient registration, inpatient admission into health care institutions, and the use of registration data in establishing and using the demographic segments of the Electronic Health Record. It also identifies a common core of information elements needed in this R-ADT process and outlines those organisational elements that may use these segments. Furthermore, this guide identifies the minimum general requirements for R-ADT and helps identify many of the additional specific requirements for such systems. It provides guidance to designers of R-ADT through a clear description of the consensus of health care professionals regarding a uniform set of minimum data elements used by R-ADT functions in each component of the larger system. |
| 10. | ISO 13606-1:2008 | Electronic Health Record communication (Part 1): Reference model | Specification for the exchange of part/entire EHR between EHR systems or between EHR systems and a centralised EHR data warehouse. It provides an information model for representing health information using UML class diagrams and the relationships among them. |
| 11. | ISO 13606-2:2008 | Electronic Health Record communication (Part 2): Archetype interchange specification | Specification for the information architecture required for inter-operability in the exchange of patients' clinical health care data between EHR systems. |
| 12. | ISO 13606-3:2009 | Electronic Health Record communication (Part 3): Reference archetypes and term lists | Definition of list of terms and the set of values that attributes in the Reference model may hold. It also defines the informative reference archetypes that correspond to the entry-level compound data structures in the Reference Models of open EHR and HL7 V3. This is to enable |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| | | | these instances to be represented in a consistent structure when communicated Using ISO 13606-3 standard. |
| 13 | ISO 18308:2011 | Requirements for an Electronic Health Record Architecture | Specification for the set of requirements for an EHR architecture to ensure EHR systems meet the needs for health care delivery, are clinically valid and reliable, are ethically sound, satisfy the prevailing legal requirements, support good clinical practices, and facilitate data analysis for various purposes.<br>While the standard does not specify the full set of requirements that are necessary in an EHR system for direct patient care or for other use cases, it contributes to the governance of EHR information within such a system. |
| **Architecture Standards** | | | |
| 14. | ISO 12967-1:2009 | Service Architecture (Part 1): Enterprise Viewpoint | Guidelines for the description, planning and development of new health care information systems, or the integration of existing ones (e.g., systems within one health care institution or across many institutions). It supports the specification of architecture that integrates the common data and business logic into a specific architectural layer, i.e., the middleware, by separating applications and making them available throughout the system in the form of services. |
| 15. | ISO 12967-2:2009 | Service Architecture (Part 2): Information Viewpoint | Specifications for the essential characteristics of the information model to be implemented by the middleware of an information system in order to provide comprehensive and integrated storage of the common enterprise data and to support the funda-mental business processes of the health care organisation, as defined in ISO 12967-1. |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| 16. | ISO 12967-3:2009 | Service Architecture (Part 3):Computational Viewpoint | Specification for the essential characteristics of the computational model to be implemented by the middleware of an information system in order to ensure a comprehensive and integrated interface to the common enterprise information and to support the core business processes of the health care Institution, as defined in ISO 12967-1. |
| 17. | ISO/HL7 1731:2006 | Reference Information Model | Specification for static modelling of health care information as viewed within the scope of HL7 standard development activities. It provides graphical representation of information requirements of HL7 version 3 standards in the form of class diagrams, use case models, state machines diagrams, and data type models. |
| 18. | ISO 21090:2011 | Harmonised data types for information interchange | Specification of data types of the basic concepts in the health care domain, the semantics of the data types using terminologies, and notations and the data types defined in ISO/IEC 11404. Presents the UML definitions of the data types, and specifies the XML representation of the data types. |
| **Structure & Content Standards** | | | |
| 19 | HL7 CDA<br>(ISO/HL7<br>27932:2009) | Clinical Document Architecture | The CDA is a standard specification for the structure and semantics of clinical documents, to support common representation of clinical documents. e.g., clinical summaries, discharge notes, and radiology reports. CDA is based on the HL7 Reference Information Model (RIM), a model of health care data consisting of generic classes from which concrete classes can be derived. It supports the use of standardised coding systems, such as LOINC and SNOMED, to enhance semantic interoperability. |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| 20. | ASTM E2369-05 | Continuity of Care Record (CCR) | This standard provides specification for the creation of patient care information documents and the exchange of such documents among health care providers. It enables a health care provider or a system to aggregate all the essential clinical demographic and administrative data about a specific patient and forward it to another practitioner or system to support the continuity of care. To ensure interoperability, the standard specifies the use of XML schema to structure an electronic CCR. The XML specification also creates flexibility, allowing users to prepare, transmit, and view the CCR in multiple ways, for example, through a browser, as an Element in a HL7 message or CDA compliant document, in a secure email, as a PDF file, as an HTML file, or as a word processing document. It also enables users to display the fields of the CCR in multiple formats. |
| 21. | ASTM E2436-05 2010 | Standard specification for the representation of human characteristics data in health care information systems | This standard provides specification for representation of the content and structure of human characteristics data for use in health care information systems. It supports inter-operability through a single, uniform representation of human characteristics at the data layer of health care information systems architecture. |
| 22. | ASTM E1744-04: 2010 | Standard Practice for View of Emergency Medical Care in the Electronic Health Record | Specification on essential information that should be documented in emergency medical care for an electronic patient record system. To ensure interoperability, the data structure specified in the standard also conforms to other American Society for Testing and Materials (ASTM) standards for the Electronic Health Record (HER). |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| 23. | HL7/ASTM CCD | Continuity of Care Document | The CCD is an integration of HL7 CDA and ASTM CCR to harmonise the data formats of these standards. It provides a set of templates for different sections of a typical summary record, for example, vital signs, family history and care plan, to facilitate reusability and interoperability. |
| 24. | HL7 CRS | Care Record Summary (Part of CDA) | A Care Record Summary document contains a patient's relevant health history for some time period. It is intended for communication between health care providers, and provides disparate hospital systems a standard format to report back to a primary care provider or other parties interested in the patient's hospital care. It is also called a discharge summary by HL7. |
| 25. | CDA for CDTHP | CDA for Common Document Types History and Physical Notes Draft Standard for Trial Use (DSTU (Part of CDA) | CDA for CDTHP is used to record information for a History and Physical Note. A History and Physical Note is a two-part medical report that documents the current and past conditions of the patient. It contains essential information that helps determine an individual's health status. The information forms the basis of most treatment plans. |
| **Security &Access Control Standards** | | | |
| 26 | ISO 13606-4:2009 | Electronic Health Record Communication (part 4): Security | This standard describes the methods for specifying access privileges to EHR data. |
| 27. | ISO/TS 21091:2005 | Directory Services for Security, Communications and Identification of Professionals and Patients | Specification for the minimal requirements for directory services in health care using the X.500 framework. It gives the common directory information and services required for secure exchange of health care information over public networks. The standard is forward-looking in that it addresses the requirements for the communication of health care information within and across health care institutions, as |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| | | | well as beyond country boundaries. It also supports a directory for identification of caregivers, health institutions and patients/consumers of health services (i.e., the Message Passing Interface (MPI). |
| 28. | ISO/TS 21547:2010 | Security Requirements for Archiving of Electronic Health Records – Principles | Specification for the basic principles required for long-term, secure preservation of health records in any format. This standard is specifically focused on document management and privacy protection issues that are related to document archiving. It defines the architecture and technology-independent security requirements for long-term preservation of EHRs by complementing ISO/TR 21548. |
| 29. | ISO/TS 22600-1:2006 | Privilege Management and Access Control (Part 1): Overview and Policy Management | Specification to support requirements for sharing health care information among independent health care providers, institutions, health insurers, patients, staff members and trading partners. It supports collaboration between several authorisation managers that may operate over organisational and policy borders. |
| 30. | ISO/TS 22600-2:2006 | Privilege Management and Access Control (Part 2): Formal Model | Specification of the underlying paradigm of formal high-level models for architectural components based on ISO/IEC 10746. It introduces the Domain Model, the Document Model, the Policy Model, the Role Model, the Authorisation Model, the Delegation Model, the Control Model and the Access Control Model. |
| 31. | ISO/TS 22600-3:2009 | Privilege Management and Access Control (Part 3): Implementations | Implementation specification for ISO/TS 22600-2:200; specifies requirements for: repositories for access control policies, and privilege management infrastructures for health informatics. |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| 32. | ISO 22857:2004 | Guidelines on Data Protection to Facilitate<br>Trans-border Flows of Personal Health<br>Information | Guidelines on data protection requirements to support the transfer of personal health data across national borders. While the standard is primarily concerned with international exchange of personal health data, it is never-theless still applicable to the protection of health information transmitted within the borders of a country (e.g., intra &inter county). |
| 33. | ISO/TS 25237:2008 | Pseudonymization | Specifications on the principles and requirements for privacy protection through the use of pseudonym services in order to protect personal health information. It defines the basis concept for pseudonymization; provides an overview of different use cases for pseudonymization (reversible and irreversible); and defines a basic methodology for pseudonymization services. It also provides a guide to risk assessment for re-identification; specifies a policy framework and minimal requirements for trustworthy practices for the operations of a pseudonymization service; specifies the policy framework and minimal requirements for controlled re-identification; and provides the interfaces for the interoperability of services interfaces. |
| 34. | ASTM E1985–98: 2005 | Standard Guide for User Authentication and Authorisation | Guidelines on mechanisms for authenticating users of health care information systems and authorising specific actions by users. The standard is applicable to both centralised and distributed environments; it defines the requirements that a single system shall meet and the types of information that shall be trans-mitted between systems to provide distributed authentication and authorisation services. It also addresses the technical specifications for how to perform user authentication |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| | | | and authorisation. |
| 35. | ASTM E1986–09 | Standard Guide for Information Access<br>Privileges to Health Information | Specification for granting access privileges to health information. It covers the requirements to keep as confidential personal, provider, and organisational data in the health care domain. It also addresses a wide range of data and data elements that are not traditionally defined as health care data, but which are essential in the provision of data management, data services, and administrative and clinical health care services. It also covers specific requirements for granting access privileges to patient-specific health information during health emergencies. |
| 36. | ASTM E2147–01:2009 | Standard Specification for Audit and Disclosure Logs for Use in Health<br>Information Systems | Specification for the design of access audit log to record all access to patient identifiable information maintained in computer systems. It includes principles for develop-ing policies, procedures, and functions of health information logs to document all disclosure of confidential health care information to external users for use in manual and computer systems. |
| 37. | ASTM E2595-07 | Standard Guide for Privilege Management Infrastructure | Definition of interoperable mechanisms to manage privileges in distributed environments, such as a service-oriented architecture environment where the security services are distributed and applications are the consumers of the distributed services. The standard also incorporates the privilege management mechanisms specified in ASTM E1986. It supports a policy-based access control mechanism, e.g., role, entity and contextual-based access control, the application of policy constraints, patient-requested restrictions, and delegation. It also supports hierarchical, enterprise-wide |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| | | | privilege management. |
| **Clinical Terminology and Classification Standards** | | | |
| 38. | SNOMED CT | Systematised Nomenclature of Medicine – Clinical Terms | Systematised Nomenclature of Medicine (SNOMED) CT is a comprehensive international and multilingual clinical terminology. It supports quality health care by enabling access to essential clinical information in a meaningful way. Each concept in SNOMED CT is organized in a hierarchy, and is linked to other concepts through relationships. This allows clinical information to be captured at the required level of detail. SNOMED CT supports cross-mapping to other clinical terminology and coding schemes, for example, the ICD-10 coding, thus enabling the reuse of coded data for purposes other than those originally intended. |
| 39. | LOINC | Logical Observation Identifiers Names and Codes | LOINC is a universal coding system for reporting of laboratory and clinical observations. Before the development of LOINC, Laboratory results that were sent electronically to health care institutions through HL7 messages used different identifiers for the same laboratory test. E.g., one laboratory system might use the identifier code"C4567" for a creatinine test, while another laboratory system might use the Code "GDTR" (or any other code) to identify the same test. This made it difficult for the receiving system to properly interpret the result and "file" it in the appropriate medical record. LOINC provides a universal coding system that supports interoperable exchange of clinical data between the laboratory system and the hospital system, so that the exchanged results can be Understood and properly interpreted. The scope of LOINC |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| | | | codes extends to cover laboratory observations (such as chemistry, haematology, Serology, microbiology, and urinalysis), as well as clinical observations (such as vital signs, intake/output, electrocardiogram, endoscopy, and obstetric ultrasound). |
| 40. | ICD-10 Codes | International Classification of Diseases | ICD-10 is an international coding system for classifying diseases, health conditions and causes of death. ICD has undergone many revisions, with the current tenth edition endorsed by the World Health Assembly in 1990, and has been implemented by member states since 1994. The ICD coding scheme facilitates compilation of vital health statistics, including morbidity and mortality, as well as for medical care reimbursement. |
| 41. | RxNorm* | RxNorm | RxNorm is a medicine terminology system developed and maintained by the United States National Library of Medicine. The database consists of the names of prescription and over-the-counter medicines available in the United States. RxNorm supports interoperability among e-Health applications through normalisation of medicine information received from multiple sources. Medicines are assigned normalised names, which consist of the component, strength and dose of the specific medicine and unique identifiers. The National Library of Medicine provides monthly release of RxNorm, with weekly updates for newly approved medicines. |
| **General IT Standards (non-health-specific)** | | | |
| 42. | ANSI INCITS 359-2004 | Role Based Access Control (RBAC) | This standard provides a mechanism for controlling users' access to computing resources based on their assigned role. It specifies the Reference Model (users, roles, permissions, |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
| | | | operations, and objects), as well as the System and Administrative Functional features of an RBAC system. |
| 43. | AES (MIOS) | Advanced Encryption Standard | The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext. |
| 44. | ISO/IEC 9075:2011 | Database Languages – Structure Query Language | ISO/IEC 9075:2011 is a multi-part standard that defines structured query language (SQL). It specifies the data structure, as well as the operations on the data stored in the structure. Parts 1, 2, and 3 of the standard are the minimum requirements for SQL, while the remaining parts define their extension. |
| 45 | ISO 19005-1:2005 | Electronic document file format for long term preservation – Part 1: Use of PDF 1.4 (PDF/A-1) | ISO 19005-1:2005 is a specification for the use of Portable Document Format (PDF) 1.4 for long-term preservation of electronic documents. |
| 46. | SOAP 1.2 (MIOS) | SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) | SOAP Version 1.2 is a lightweight protocol intended for exchanging Structured information in a decentralised, distributed environment. "Part 1: Messaging Framework" defines, using XML technologies, an extensible messaging framework containing a message construct that can be exchanged over a variety of underlying protocols. |
| 47. | XML V1.0 (MIOS) | Extensible Markup Language (XML) 1.0 (Fifth Edition) | The Extensible Markup Language (XML) is a subset of SGML that is completely described in this document. Its goal is to enable generic SGML to be served, received, and processed on the Web in the way |

| No. | Standard | Title | Abstracts |
|---|---|---|---|
|  |  |  | that is now possible with HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML. |

## 4.0 List of Reviewers

| | | |
|---|---|---|
| 1 | John Muthee | Savannah Informatics |
| 2 | Naomi Shiyonga | MOH |
| 3 | Leonard Njeru | Murang'a District Hospital |
| 4 | Dr. David Soti | MOH |
| 5 | John Mwihia | MOH |
| 6 | Sarah Chuchu | MOH |
| 7 | John Kabanya | MOH |
| 8 | Rachael Wanjiru | MOH |
| 9 | Robert Wathondu | MOH |
| 10 | Onesmus Kamau | MOH |
| 11 | Charles Kinuthia | MOH |
| 12 | Anne Barsigo | MOH |
| 13 | Paul Malusi | MOH |
| 14 | Paul Karimi | MOF |
| 15 | Washington Anyango | MOF |
| 16 | Josphat Kiongo | KNH |
| 17 | Samuel Kanga | I-TECH |
| 18 | Mwenda Gitonga | Futures Group |
| 19 | Brian Wakhutu | Futures Group |
| 20 | Anne Koimur | Egerton University |
| 21 | Liliana Asumpta | Egerton University |
| 22 | Andrew Mukaru | Egerton University |
| 23 | Jairus Musumba | CCN |
| 24 | David Muturi | AfyaInfo |
| 25 | Tony Munuhe | Private Contributor |

## 5.0 Works Cited

Accenture2015 */us-en/health-industry-index* Available at:https://www.accenture.com10January2015

AfyaInfo Project Kenya2013*http://www.afyainfo.org/index.php/features/the-afyainfo-project* Available at:http://www.afyainfo.org/index.php/features/the-afyainfo-project03January2014

DHIS, DSRS2010*Implementation Guide*eGovernment, Directorate of2010-2014*Kenya Strategic Plan*

Government Of Kenya *Kenya Health Information System* Available at:https://hiskenya.org/dhis-web-commons/security/login.action 23May2013

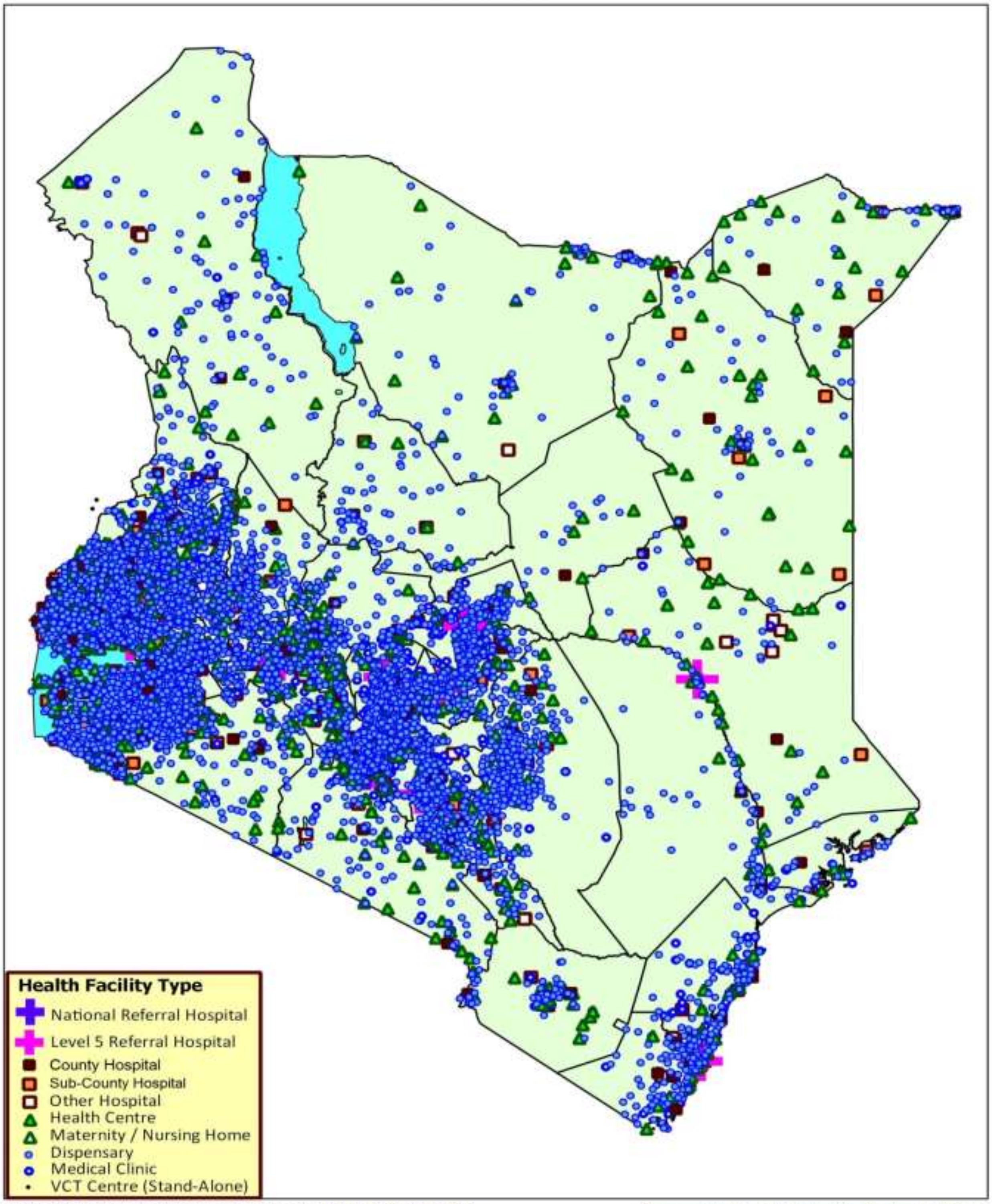
Government of Kenya*Master Facility List*Available at:http://www.ehealth.or.ke/facilities/23May2013

Healthcare Information and Management Systems Society 2015*www.himss.org/* Available at:http://www.himss.org/2015

Repulic of South Africa2014*National Health Normative Standards Framework for Interoperability in eHealth in South Africa*South AfricaCSIR GWDMS Number: 240075

U.S. Department of Health & Human Services2014*www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html* Available at:http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html10January2015

## County Health Facility Distribution by Type
## KENYA



SOURCE: MASTER FACILITY LIST (MFL) www.ehealth.go.ke

Prepared by USAID AfyaInfo Project (c) 2013

USAID
FROM THE AMERICAN PEOPLE

PEPFAR