
MINISTRY OF MEDICAL SERVICES

MINISTRY OF PUBLIC HEALTH AND SANITATION

# Kenya Standards and Guidelines for E-Health Systems Interoperability

March 2014



**March 2014**

**Recommended Citation:** Government of Kenya. 2013. Kenya Standards and Guidelines for E-Health Systems Interoperability. Nairobi, Kenya: Ministry of Health, AfyaInfo Project.

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, the University of Oslo, Knowing Inc., the Kenya Medical Training College, 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.



AfyaInfo
Kenya National HMIS Program

# Table of Contents

# List of Acronyms

| | |
|---|---|
| CHMT | County Health Management Team |
| EHR | Electronic Health Record |
| HIS | Health Information System |
| HL7 | Health Level 7 |
| ICT | Information and Communication Technology |
| SDMX-HD | Statistical Data and Meta-data Exchange for Health Domain |

# Foreword

The Ministry of Health recognises the value of the application of Information and Communication Technology (ICT) system interoperability standards and guidelines as a means of enhancing efficiency and effectiveness in the delivery of health services. ICT system interoperability standards and guidelines have the potential to impact upon almost every aspect within the health sector. In public health, system interoperability standards and guidelines for information management and communication processes are pivotal, and public health activities are facilitated or limited by the availability of those standards and guidelines.

The implementation and use of such standards initially adopted a diversified approach, where the implementers worked in a relatively autonomous fashion, without any reference to a common set of system interoperability standards and guidelines, and with no common operating platform and standards. This approach has led to duplication of efforts, lack of interoperability, and inappropriate use of ICT resources, which has made it difficult to effectively and efficiently use ICT to deliver health care services.

As the Ministry of Health 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 and standardised system interoperability. The Ministry recognises the need for a consistent approach to the use of ICT systems and, thus, the need to formulate these Standards and Guidelines.

The standards and principles set out in this document shall be applicable in the health sector to those involved in offering services or information to the public. This document provides guidance and a consistent approach across the health sector for establishing, acquiring and maintaining current and future information systems and ICT infrastructure that foster interoperability across systems.

This document was developed through a participatory process involving all stakeholders in health, including government ministries/agencies and development partners, and is based on internationally recognised best practice principles. It was created in consultation with a vast array of subject experts and interest groups, with input from all Government Ministries, Departments and Agencies. The standards and principles contained herein borrow from e-Government standards. They shall be used in accordance with ICT standards, system interoperability principles, and Ministry of Health policy and strategy, and shall be reviewed and updated regularly as needed.

It is my sincere hope that all the actors in health will rally around these standards to ensure that we all steer the country towards the use of acceptable standards.

Dr. Francis Kimani
Director of Medical Services

# Acknowledgements

The realisation of these System Interoperability Standards and Guidelines has been achieved through tremendous efforts and commitment of various individuals and organisations.

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, Professor Segor, whose enormous support and guidance led to the finalisation of the document.

Dr Francis Kimani, 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 John Masasabi, the Head, Directorate of Policy, Planning and Health Care Financing, and Dr David Soti, Head, Health Informatics Monitoring and Evaluation.

The process received tremendous technical and financial support from our partners: the AfyaInfo Project (funded by USAID), and ITECH. Special thanks go to Dr Martin Osumba, Raphael Pundo, David Muturi, Solomon Simba, Erastus Mburu of AfyaInfo, and Sam Kanga of ITECH Kenya.

Special thanks also go to Dr Muthami, the Head of the Health Information System (HIS) Unit, Onesmus Kamau, Ag. Head E-health Unit and staff members Francis Gikunda,Jeremiah Mumo, Nancy Amayo,Ann Gitungo, Esther Kathini, Margaret Chiseka, Robert Wathondu, Omondi, Abdullahi Kimogol, Dorcas, Peres, Joseph Macharia, Aurelia, and Gladys for their valuable contributions to the entire process of the development of this document.

Thanks are also due to ICT staff James Njiru, Rachael Wanjiru and Nicholas Ngari for their steadfast contribution to the realisation of this 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.

# Authority

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 HIS Policy (2013-2030)
7. Kenya Health Policy Framework (2012-2030)
8. Health Sector ICT Standards and Guidelines ( 2013)

## Vision Statement

The vision of e-Health is to have effective, efficient, accessible, equitable, and secure consumer-friendly health care information systems, infrastructure, and applications for improved health care services in Kenya.

## Mission Statement

To provide and promote use of highly effective, reliable, and innovative information systems to support clinical decision making, patient management, and health care research to improve health care services in Kenya.

## Objective

- To support more-informed policy, investment and research decisions through access to timely, accurate and comprehensive reporting on Kenyan health system activities and outcomes
- To improve the quality, safety and efficiency of clinical practices by giving care providers better access to consumer health information, clinical evidence and clinical decision support tools
- To enable the Kenya health sector to be more effectively operated as an inter-connected system, overcoming the current fragmentation and duplication of service delivery
- To create linkages between health research and information technologies

## Scope

- Community-Based Information Systems
- Primary Health Care Information Systems
- Hospital Management Information Systems
- Diagnostic and Imaging Services Information Systems
- Telemedicine and E-Learning Information Systems
- Population and Public Health Surveillance Information Systems
- Health Care Insurance and Medical Schemes
- Supply Chain and Logistics Information Systems
- Human Resources for Health Information Systems
- Integrated e-Health Architecture and Standards
- Unique Identifier and Integration with National Identity Department

## Key Principles

1. Strong leadership and governance
2. Collaboration and partnerships for shared information and services among stakeholders
3. Leveraging available human, financial and technical resources
4. Safeguarding health care service integrity, client confidentiality and secure information interchange
5. Harmonizing and coordinating disparate health and information technology expertise
6. Phased implementation of prioritized e-Health initiatives in line with the strategic framework
7. Redundancy in mission-critical aspects of e-Health systems

# 1.0 Data Exchange Standards

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

a. Aggregate Data Standards, e.g., Statistical Data and Meta-data Exchange for Health Domain (SDMX- HD)

b. Clinical data standards, e.g., Health Level 7 (HL7), Logical Observation Identifiers Names and Codes

c. Administrative data standards

d. Imaging standards, e.g., Digital Imaging and Communications in Medicine, picture archiving and communications system

## Methods of Exchange

System owners should 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.

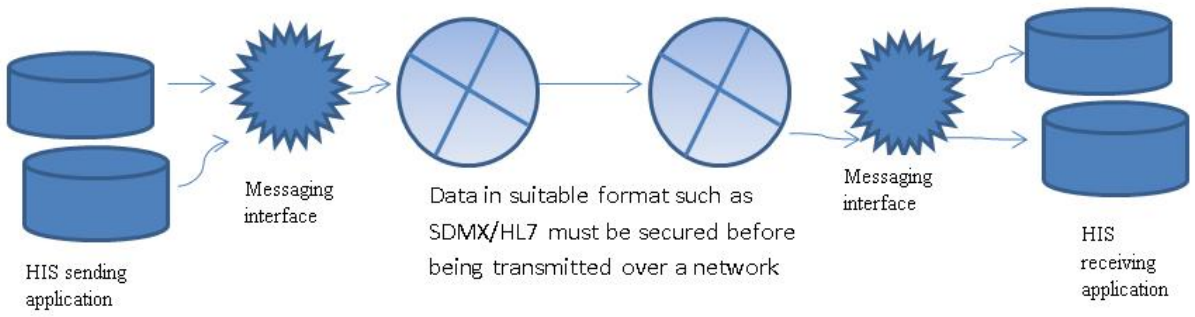
### a. Manual

Domain-specific data exchange templates shall be provided by system owners who implement manual modes of transferring data between systems. These system owners are responsible for ensuring sufficient levels of documentation to enable the exchange of data between different systems.

### b. Automated

Various methods can be used for automated data exchange. These include the Application Programming Interface, agents, and "middleware." It shall be the responsibility of system owners to implement an automated messaging interface for their systems. However, all systems with an automated data exchange format shall share data in Extensible Markup Language format.

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



## Data Types' 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.

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

| | |
|---|---|
| Height | Meter |
| Weight | Kgs |
| Temperature | Degree Celsius |
| Blood pressure | Mm/hg |
| Blood sugar | Mmol/l |
| Blood group | Rhesus factor |
| Mid-upper arm circumference | Centimeters |
| Dates e.g. date of birth | dd/mm/ yyyy |

## Unique Identifiers

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

### a. Patient Identifiers

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

I) National unique patient identifier

II) Patient names in full

III) Gender

### 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. Service Provider Identifiers

Service provider identification 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. Service provider identifiers during data exchange shall include:

I) Professional Registration Certificate number or license number

II) Area of specialization

## 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.

### a. Community to Facility

Systems at this level exchange the following data:

I) Referrals

II) Commodities and supplies

III) Demographic data

IV) Epidemiological data

### b. Within a Facility

The systems within a health facility exchange the following data:

I) Order entries – these include: laboratory orders, prescription orders, commodities and supplies

II) Patient movements between the wards and departments

### c. Facility to Facility

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

I) Referrals

II) Commodities and supplies

III) Electronic consultations

### d. Facility to County (Administrative)

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

I) Aggregate data

II) Commodities and supplies data

III) Electronic consultation

**e. County to National**

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

I) Aggregate reports

II) Data on commodities and supplies

III) Electronic consultations

# 2.0 Information Security Standards and Guidelines

## 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-based or aggregated, but irrespective of that it must be safeguarded. In developing health sector ICT standards and guidelines it was found that the most health care data is generated at the health facilities and shared with other levels of the health care system. This sensitive data should be protected by policies, rules and regulations to safeguard it from losses and misuse. It is transmitted using manual or electronic forms/modes; in either case it is imperative that health information systems should have clear standards that guide how data is captured, accessed, stored, modified, transmitted, and archived/destroyed.

Ensuring 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 could have life-threatening consequences.

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

## Security rules to govern data exchange

### Administrative safeguards

These safeguards aim at protecting the confidentiality 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 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 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 shared confidentiality is only practiced in the interest of the patient.

Persons or entities implementing health information systems must ensure adherence to the Ministry of Health HIS policy 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 ICT standards and guidelines on security in the management of data, server rooms, and information system components.

### Physical safeguards

These safeguards control physical access to the data managers' offices and computer systems. The required physical safeguards include:

- The parties exchanging data should agree on the most secure way to exchange data (manually move the data in external storage devices, or use the VPN) and have a mitigation plan in case the transmission channel is compromised.
- Restrict data exchange to formats that are defined by this document on e-Health interoperability standards.
- Install facility access controls, such as locks and alarms, to ensure only authorized personnel have access to facilities that house systems and data.
- Ensure 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.
- Implement workstation use policies to ensure proper access to and use of workstations.

### Technical safeguards

These safeguards include hardware, software, and other technology that limits access to electronic information.

The required technical safeguards to be adhered to by all implementers and developers of health information systems include the following:

- 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

## Health Information Privacy

It is important to ensure that the privacy of individuals' medical records and other personal health information is maintained, so it is important to ensure that the HIPAA privacy rule on protected medical information – borrowed from the U.S. Department of Health and Human Services and adopted as part of these e-health standards and guidelines for interoperability – is strictly followed. This rule proposes civil and criminal penalties for any violations.

The tenets of HIPAA that have been borrowed and used as part of the 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.

In addition, patients have individual legal rights to access their health information and learn about disclosures of their health information, unless on special occasions. Their health care provider should take the responsibility for respecting these rights.

As a covered entity, one has responsibility to the patients under the stipulated regulatory Privacy Rule, including:

*Notice of Privacy Practices:* Under the Privacy Rule, covered entities must provide patients with full information on how their protected health information is used and disclosed. This is accomplished by giving patients a Notice of Privacy Practices that describes how an individual's information may be used or shared, and which specifies an individual's legal rights with respect to his or her protected health information held by the covered entity (many of which are described below), and the covered entity's legal duties.

**Protected Health Information**

The Privacy Rule establishes national standards to protect individuals' medical records and other personal health information, and applies to health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

All entities and persons implementing Health Information Systems must also ensure and implement mechanisms to trace information alteration, and to monitor information on transit detection mechanisms. There should be intrusion detection mechanisms that trace data entry, storage, transmission, and data exchange activities. Any information that is transmitted should have an audit trail log on the exchange process and highlight the users' information and type of information transmitted. The system developer, implementer, and owner are responsible for ensuring that the security mechanisms are in place.

The mechanisms adopted by persons and entities that participate in a network for the purpose of electronic exchange of individually identifiable health information should address:

(1) Monitoring for internal compliance, including authentication and authorizations for access to or disclosure of individually identifiable health information

(2) The ability to receive and act on complaints, including taking corrective measures

(3) The provision of reasonable mitigation measures, including notice to individuals of privacy violations or security breaches that pose substantial risk of harm to such individuals

It is important to note that the Privacy Rule establishes a set of national standards for the use and disclosure of individually identifiable health information – often referred to as protected health information – by covered entities, as well as standards for providing individuals with privacy rights and helping individuals understand and control how their health information is used.

**Privacy Rule requirements:**

- Apply to most health care providers, including those who do not have EHRs
- Set standards for protecting individually identifiable health information across all media (electronic, paper, and oral)
- Limit how covered entities may use and disclose individually identifiable health information they receive or create
- Give individuals rights with respect to their protected health information, including a right to examine and obtain a copy of information in their medical records, and the right to ask covered entities to amend their medical record if information is inaccurate or incomplete
- Impose administrative requirements for covered entities, such as training of employees with regard to the Privacy Rule
- Establish civil and criminal penalties

**A covered entity shall have responsibilities to patients including:**

- **Patient access to their information:** Patients have the right to inspect, review, and receive a copy of health information about themselves held by covered entities or business associates in a designated record set, which includes a health care provider's medical and billing records. Generally, these health plans and providers have to comply with requests for access within 30 days.
- **Amending patient information**: Patients have the right to request that covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete. If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendments to persons identified by the individual as having received the original information and being in need of the amendment(s), as well as to those entities that the covered entity itself identified as having received the original information who would be in need of the amendments due to their prior or foreseeable reliance on the original information to the detriment of the individual. If the request is denied, covered

entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record.

- **Accounting of disclosures**: Individuals have a right to receive an accounting of disclosures. Accounting is required for certain disclosure purposes only. A covered entity must provide an accounting of disclosures made during the accounting period, which is six years immediately preceding the accounting request, but a covered entity is not obligated to account for any disclosure made before its Privacy Rule compliance date.
- **Rights to restrict information:** Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment, or health care operations; disclosure to persons involved in the individual's health care or payment for health care; or disclosure to notify family members or others about the individual's general condition, location, or death. A covered entity is under no obligation to agree to requests for restrictions; however, a covered entity must have a procedure to evaluate all requests. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.

Protected health information can be in any form – electronic, paper, or oral – and includes financial and demographic information collected from patients.

The risk analysis process will lead medical and administrative staff one to systematically examine many aspects of their medical practice:

- EHR software and hardware
- Adequacy of their practice protocols
- Physical setting and environment
- Staff education and training
- EHR access controls
- Contracts with their business associates
- Patient relations and communications

# 3.0 System Data Quality and Reliability, and Performance Standards and Guidelines

## System Data Quality

Aspects of system data quality:

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

- Standardized data elements across systems participating in National Health Information Survey (NHIS) published Metadata dictionary.
- Repository of validation rules that enforce business processes and comprehensive data cleaning procedures. (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 robust data cleaning procedures.)
- Develop and enforce (automatic) tools that use business rules to reference data in order to analyze and rank data according to completeness, conformity, consistency, duplication, integrity and accuracy.

## System Reliability and Performance

✓ Hardware

a. Reliable hardware as per international and ICT standards

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

c. Reference Data Centre guidelines

✓ Human resource

a. Data Centre guidelines

b. Ministry of Health ICT standards

✓ Software

a. Data Centre guidelines enshrining standard software engineering metrics

b. Security standards

✓ Communication hardware and software

a. Connectivity to servers available at 99.9%

b. Security standards

## Data Governance: –An Enhancement Framework For NHIS

**Data governance** is a set of processes that ensure that important data assets are properly managed throughout the enterprise. Data governance ensures that data can be trusted and that people can be made accountable for any adverse event that happens because of low-quality data. It is about putting people in charge of fixing and preventing issues with data so that the enterprise can become more efficient. Data governance describes an evolutionary process for an organisation, altering the entity's way of thinking and setting up the processes to handle information so that it may be used by the entire organisation. It's about using technology when necessary.

Data governance is also a quality control discipline for assessing, managing, using, improving, monitoring, maintaining and protecting organisational information. It is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models that describe who can take what information under what circumstances, using what methods.

**The goals of data governance in the NHIS:**

- Increasing consistency and confidence in decision-making
- Decreasing legal liability
- Designating accountability for information quality
- Enabling better planning by supervisory staff
- Minimising or eliminating re-work
- Establishing process performance baselines to enable improvement efforts

## Key Elements of The NHIS Data Governance Framework

### Availability

The data must be available to the applications of all NHIS users when needed.

### Accessibility

Data is accessible regardless of the application used.

### Interoperability

The data must be both semantically and syntactically interoperable within and across systems.

### Auditability

There must be a trail of the data from its source to its destination.

### Quality

The data must be timely, accurate and complete.

### Security

The data must be kept secure.

## Policies

*Standards*

All data definitions, structures, formats and taxonomies must be included within a policy in order to facilitate interoperability. These will be encapsulated within the Enterprise Architecture.

*Organisation*

These are the roles and responsibilities for each individual within the NHIS. These must be defined. Of particular importance are the roles of data producers, verifiers, approvers and data consumers.

*Processes*

These are the processes around the creation, development and management of data including business logic rules as well as access and monitoring mechanisms.

*Issue Management*

There must be data management policies that govern data prioritisation and remediation. These will exist in the form of protocols, Standard Operating Procedures, etc., in the current HIS structure specific to the NHIS.

## Contracts

Additionally there is a need to lay out policies that govern the appropriate use of data by stakeholders who participate in the NHIS. These will be formal contracts whose detail entails the following.

*Data requirements* – The data used within the NHIS is mapped to a specific requirement, with rules established to measure compliance.

*Data management* – Data policies are defined and documented for common datasets within the NHIS.

*Data validation* – Validation methods are embedded into each of the defined business processes. The methods are aided by technology but are not limited to technology-based validation, but may be extended to physical validation via human intervention.

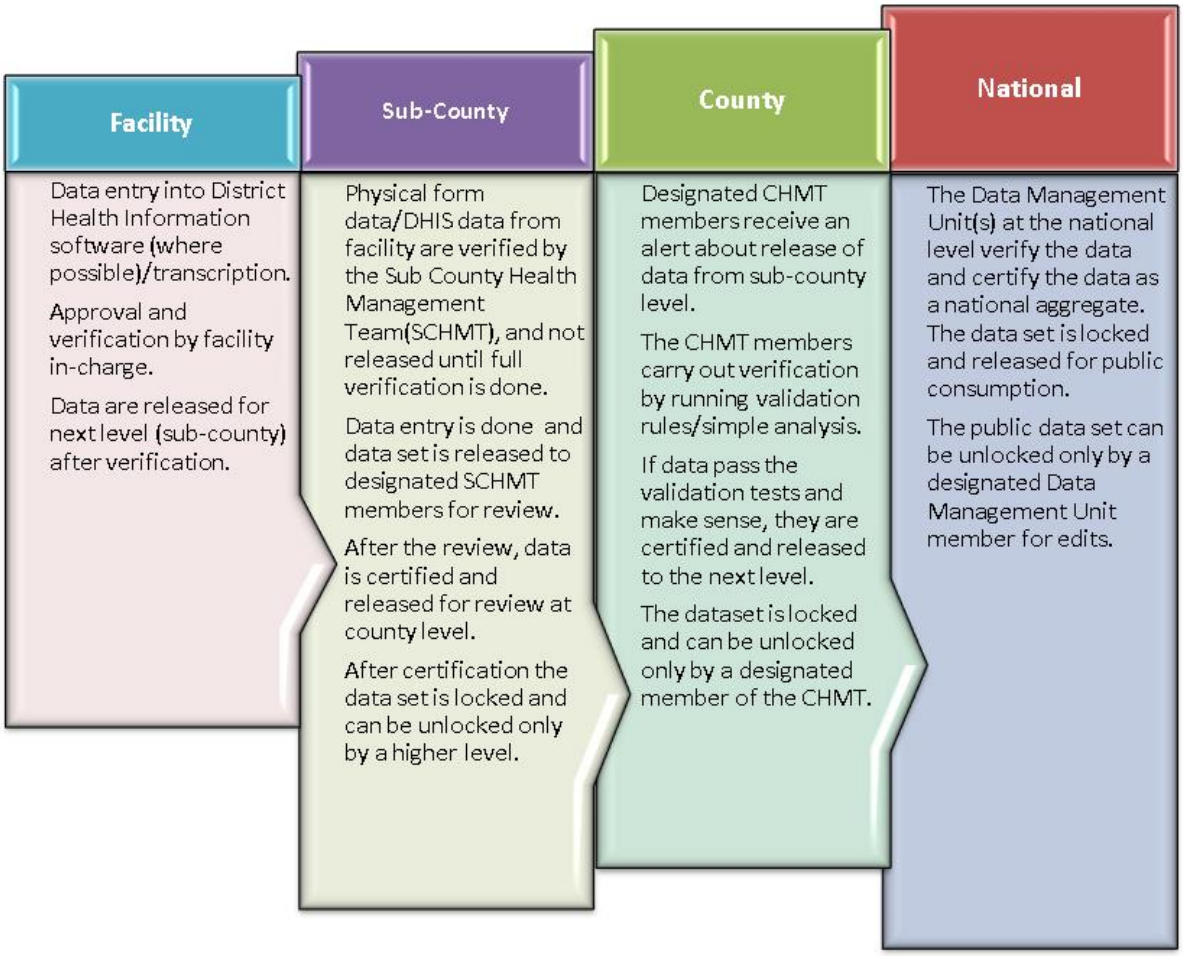
*Alerts and remediation* – Processes for prioritising data issues and methods of remediation and the responsibilities of each of the stakeholders are defined. These may be physical methods or technology-based processes.

## Proposed Data Governance Structure to the NHIS

### Policies

Kenya's federated governance structure means that there is autonomy at the county level. The national level (State Department of Health) will formulate policies regarding health data, i.e., Standards, Organisation, Processes and issue management. The County Department of Health is charged with the autonomous implementation of the national policies. In this structure there is need to encapsulate intermediate verification and approvals as the data flows upwards, from the facilities, to sub-county levels, to county levels, and eventually to the national level in the form of a policy.

## Intermediate verification and approval



This will be a feature in built into the NHIS, where at each level of aggregation data are verified by a designated member of the County Health Management Team (CHMT) or the entire CHMT. After verification the data will then be certified for release to the next level.

## Reporting timelines

- Verification at the facility should be done by the 4th of the month.
- Reporting from facility to sub-county level should be done by the 5th.
- Verification and approval by sub-county level should be done by the 7th.
- Data entry at both the facility and sub-county should be done by the 15th.
- Verification of data entered at the sub-county level should be done by the 17th.
- Locking of facility datasets at the sub-county level should be done by the 20th.
- Verification, approval and locking of individual datasets per facility at the county level should be done by the 25th.
- Verification and remediation at the national level should be done by the 30th.