KENYA DIGITAL HEALTH SOLUTIONS CERTIFICATION FRAMEWORK

Draft February 2024

Commented [1]: Include Business intelligence as part of the certification framework

Commented [2]: As part of the certification framework, a system must be able to access the workforce registry to ensure that the profiles created are for those who are duly licensed to perform .

MINISTRY OF HEALTH

Table of Contents

Foreword

Commented [3]: Update this section once the entire document has been completed

The Health Information System (HIS) strategic plan of 2009–2014 advocated for integration of the various subsystems of the HIS with reference to national and international standards. Accordingly, the Ministry of Health (MoH), supported by its implementing and development partners, revised the initial Electronic Medical Record Standards and Guidelines to include Primary Health Care, Pharmacy Information Systems Standards and Guidelines, Laboratory Information Systems Standards and Guidelines, and Health Information and Communication Technology (ICT) Standards and Guidelines.

These documents addressed various challenges, including: varying functionality and data security; inability of the HIS to communicate, leading to silos of information; inability to meet MoH reporting needs; and unpredictability of support from system vendors. The documents went on to define the essential minimum data sets and functionality that should be captured by the systems in order to support the provision of quality health care services, as defined by various clinical practice guidelines; and the need for these systems to communicate for purposes of sharing patient information, among other things.

The Standards and Guidelines documents provide a benchmark against which the HIS can be regulated to ensure that it meets the needs and requirements of the various MoH stakeholders. To facilitate easy interpretation of the document, the MoH, supported by implementing and development partners, have packaged these documents into the Certification Framework. The framework is a living document, and will grow as additional Standards and Guidelines become available, or existing guidelines are revised.

The framework targets system owners and developers, and seeks to provide a tool for self-attestation by the target groups to gauge their level of conformance to the Standards and Guidelines before they make formal application to the MoH for certification of their systems. The framework defines specific processes that a system would be subjected to, based on whether it is an existing or an emerging system. The framework provides a scoring methodology, under which systems are required to score 100% to be certified in their respective domains.

I hereby call upon county governments to require the owners of both existing and emerging health systems to present their systems to the certification committee for certification, as per the provided guidelines. This will ensure realisation of standardised systems that will, among other things, exchange patient data, enforce completeness of data through various validation routines, and support comparability of health data generated by different systems.

I wish to thank the task force, shepherded by the MoH Division of Health Informatics, Monitoring and Evaluation, which held numerous deliberations in consultation with health sector stakeholders towards the realisation of this key national document. Your input will go a long way to ensuring quality health care provision in an age where national and county governments have moved to embrace the use of ICT in health care.

____

[name]
Director of Medical Services

- # Definitions

  - ## Abbreviations and Acronyms

CB	Certification Body
CCK	Communications Commission of Kenya
CHMT	County Health Management Team
CHRIO	County Health Records Officer
DHA	Digital Health Agency
DHS	Digital Health Solution
DPA	Data Protection Act
DPIA	Data Protection Impact Act
EHR	Electronic Health Record
EMR	Electronic Medical Record
HIS	Health Information System
HRMIS	Human Resource Management Information System
ICT	Information and Communications Technology
ICTA	Information and Communications Technology Authority
IDSR	Integrated Disease Surveillance and Response
IGC	International Growth Centre
IHR	International Health Regulations
IT	Information Technology
JKUAT	Jomo Kenyatta University of Agriculture and Technology
KEBS	Kenya Bureau of Standards
MoH	Ministry of Health
PAS	Patient Administration System
SHA	Social Health Authority

○ Terms

Health Information System

Any electronic system that captures, stores, manages, and/or transmits data related to public health, or to activities within the health sector. Among the systems in this category:

- Electronic medical records (EMRs)
- Electronic health records (EHRs)
- Primary care systems
- District-level routine information systems
- Disease surveillance systems
- Pharmacy information systems
- Laboratory information systems
- Hospital patient administration systems (PAS)
- Human resource management information systems (HRMIS)

System Owner

The individual or institution responsible for the procurement, development, integration, modification, operation, and maintenance of an information system. Ownership is transferrable when the product is sold.

System Vendor

An individual, institution, or company whose principal product is a health information system targeted for use in the Kenyan health sector. May be used interchangeably with **system owner** if the vendor owns the product.

Testing Laboratory

A designated facility for testing individual IT systems. The testing includes black-box functional testing, as well as regression testing, load testing, installation, usability, and security testing.

Testing Tool/Script

A set of instructions (written using either a scripting or natural language) performed on an information system under test conditions to verify that the system performs as expected and meets minimum requirements.

System Users

These include Social Health Authority (SHA), Hospitals, Health Care Providers, System Developers and others seeking to have their system certified

Digital Health Solutions

Commented [4]: This section needs to be completed

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Commented [5]: Provide a definition of this

Formatted

Formatted

Formatted

1 Introduction

Health information systems (HIS) in Kenya include a broad range of information and communication technology (ICT) applications used in the delivery of health care services, such as:

- Hospital management and information systems
- Electronic patient records
- Knowledge-based and expert systems
- Clinical decision support systems
- mHealth systems
- Laboratory systems
- Pharmacy management systems
- Radiology systems
- Telemedicine

When properly utilized in a coordinated setting, these systems are instrumental in improving coordination of care, advanced clinical processes, data capture and sharing, and population health outcomes, as well as informing health policy.

Health information systems have been implemented in such countries as Australia, the UK, New Zealand, and Canada. These countries established national e-health initiatives requiring implementation of HIS and electronic health records (EHRs), coupled with protection of the privacy and confidentiality of such records.

In addressing new opportunities to implement health information systems for the purpose of improving health outcomes, we appreciate that different parts of the sector have different information-systems capabilities. These differences call for supporting the advancement of less-developed systems, while at the same time allowing the more capable or advanced systems to continually innovate. Therefore, as this certification framework is developed, our approach should be to accommodate these inequalities by providing sets of minimum or baseline criteria that must be met by all systems.

To develop a reliable and secure HIS, we must ensure that the appropriate information security mechanisms are built into it, in order to guarantee the security and availability of highly sensitive health information. Uniform standards must be put into place to enable safe, accurate, and timely exchange of health information. Without such standards, the abbreviations, codes, terms, and processes used by one service provider may differ from those used by another provider. Standards already exist in most of the health sector, serving as a vital component in building systems that allow us to share information effectively—but barriers still exist, as different systems use different versions of the same standards, address different portions of the standards, and/or interpret the standards differently.

Independent health information technology (IT) evaluation schemes are critical in assessing HIS compliance. Evaluation criteria established through collaborative initiatives provide benchmarks for assessing the degree of compliance by systems, both those in the market, and those already in use.

Commented [6]: Update this section once the document has been completed

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

This document sets out the policies that govern the certification process; these policies define what is to be certified, what it means to be certified, and the process for achieving and maintaining certification. It is intended primarily for suppliers and vendors who would like to have their HIS products certified, but it can also be used by certification bodies as a benchmark tool during the certification process.

Formatted: Font color: Red

2 Certification Framework

2.1 Criteria

A certification framework is driven by several things: the standards or criteria to be met, industry expectations, and audience needs~~A certification framework is driven by the standards or criteria to be achieved, industry expectations, and audience needs~~. This framework defines the policies that govern the operation of the Digital Health Solutions/Interventions ~~HIS~~ certification process~~gram~~. These policies set forth under this framework act as a guide for Kenya Digital ~~-~~Health Agency, users, vendors, and developers on the requirements and specifications for progression through the certification process. They define what can be certified, what it means to be certified, and the process for acquiring and maintaining certification. They also define the obligations of the Digital Solution/Intervention~~HIS~~ being certified to meet applicable conformance requirements.

Commented [7]: Plenary

Commented [8]: Define users

This document is intended primarily for digital health solutions providers ~~vendors~~ seeking to have their systems certified, and guide ~~but~~ buyers and users to know ~~will what to expect from digital he also find this document useful for understanding what to expect~~ from a certified Digital Health Solution/Intervention~~HIS~~.

Certification indicates that the Digital Health Solution/Intervention~~HIS~~ meets established health-sector standards,- Health Act 2017, Digital Health Act 2023, Data protection Act 2019, and complies with all other relevant laws and regulations~~requirements~~.

This certification framework focuses on four main criteria:

- Functionality
- Reporting and Alerts
- Security, Privacy, and Confidentiality
- Information Exchange and Interoperability

2.1.1 Functionality

The **functionality criteria** define the range of operations and/or services that the Digital Health Solution/Intervention~~HIS~~ should be able to run without significantly compromising the objectives of existing~~HIS~~ regulations. These criteria focus on patient care and service delivery as components in meeting the objective of improving quality of care. They apply to all digital health solutions/interventions ~~systems handling EHRs~~, including (but not limited to) hospital information systems, community health solutions, pharmacy information systems, laboratory information systems, mHealth, digital health apps, radiology information systems, logistics management systems, claims management systems, human resources for health systems, clinical decisions support systems and referral tracking systems; ~~and cover the following categories:~~

- ~~Patient demographics and administrative information~~

Formatted: Space After: 10 pt, No bullets or numbering, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border)

  - ~~Provider information~~
  - ~~Patient list management~~

- ~~Patient unique identification*~~
- ~~Problem lists*~~
- ~~Allergy information~~
- ~~Medication list~~
- ~~Results access and view~~
- ~~General ordering requirements~~
- ~~Clinical provider order entry~~
- ~~Ordering: medication orders~~
- ~~Medication reconciliation~~
- ~~Decision support for medication and immunization orders~~
- ~~Administration of medication, immunization, and blood products~~
- ~~Decision-making support for administration of medication, immunization, and blood products~~
- ~~General clinical decision support*~~
- ~~Clinical task management~~
- ~~Capture of patient-originated data*~~
- ~~Health records management~~

2.1.2 Reporting and Alerts

These criteria include the policy guidelines and standards that support routine reporting and notification for public health emergencies of~~and~~ reportable conditions or diseases. They aim to strengthen the routine reporting requirements entrenched in the Integrated Disease Surveillance and Response (IDSR) reports and required by international health regulations (IHR). Notifications submitted to the MoH and National Public Health Institute~~other public health agencies~~ (including emergency operation centres) are a key component of any Digital Health Solution/Intervention~~HIS~~. Additionally, immunisation registries, civil registries, and other ~~disease~~ registries should be capable of receiving reports from the Digital Health Solution/Intervention~~HIS~~. Ad-hoc reports for strategic planning within the county and national health systems are also a requirement. t

Reporting requirements include:

- Immediate reportable diseases
- IDSR reporting (weekly and monthly)
- Public health events
- Diseases or events of international concern
- Registries
- Routine reporting
- Shared Health Record
- Client registry

Commented [9]: reporting should be near real time @wogherax@gmail.com _Assigned to wogherax@gmail.com_

Commented [10]: Do we need to mention the periodicity

2.1.3 Security, Privacy, and Confidentiality

These criteria include policies governing the securing of sensitive personal –level health information, system access controls, role-based user authentication, data-integrity issues, encryption~~encyrption~~ , data minimization, data retention audit trails, and ~~adhere~~adherence~~adherance~~ to the Data ~~p~~Protection ~~a~~Act, 2019~~other related measures~~. The aim is to ensure compliance with international and national regulations for securing personally identifiable information and digital health interventions ~~electronic health records~~ against unauthorised access. They include criteria for regulating:

- Integrity of patient records
- Access to health records, and financial and transactional information
- Data sharing
- Legal documents
- Data Back-up and recovery policies

2.1.4 Information Exchange

Commented [11]: Implementation guide for FHIR...

These criteria address the ability of systems to share or transfer information across systems, independent of platform, using standard data formats and common infrastructure practices. This should comply with the Kenya Health Information Systems Interoperability Framework and should be able to exchange data seamlessly with Kenya National Health Information exchange (Kenya Digital Health Superhighway) in compliance with the Data Protection Act 2019, and the Digital Health Act 2023 .With common data standards, health information systems can exchange information more efficiently to meet the broad scope of data collection and reporting requirements. These criteria cover the following:

- **Definition of core data elements:** determination of the data to be collected and exchanged.
- **Core data interchange formats:** interchange standards and document architectures for structuring data elements as they are exchanged e.g. HL7, SDMX-HD, ~~Apache Camel etc~~.
- **Terminologies:** the medical terms and concepts used to describe, classify, and code the data elements, and the data expression languages and syntax that describe the relationships among terms/concepts.
- **Knowledge representation:** standard methods for electronically representing medical literature, clinical guidelines, and the like for decision-making support.

In each of these four areas, the criteria are clearly defined, with time frame~~timeframes~~ on when the requirements should be met by already existing or running systems. The framework also defines specifications and criteria that are:

a) **Required** (MUST/SHALL): requirements that *all* systems *must* meet in order to be certified.
b) **Recommended** (SHOULD): requirements that certified systems *should* have, but are given a specific amount of time to adopt or implement. After the grace period, they *must* be implemented.

c) **Optional** (MAY): specifications that are not mandatory, but desirable.

2.2 Certification Governance Structure

~~2.2.1~~ Certification ~~Panel/Committee~~

2.2.1 The Digital Health Agency shall publish and enforce the certification framework in doing this they will:

Commented [12]: to make a consideration not to stifle innovation by making accessibility too hard for pilots/research; whilst maintaining strictness for interacting with patients and patient data and the ability to access the shared services with the HIE

- Provide oversight of the certification process.
- support the Review, ~~authorise~~, and publishing of the Digital Health standards and guidelines.
- Disseminate standards and guidelines, and the certification framework.
- Develop test methodologies, test data, and scripts.
- Review and revise test methodologies and plans.
- Provide arbitration services on contentious issues.
- ~~Review and improve the certification framework every three (3) years.~~

In the process of certification the DHA will:

- Receiving and reviewing applications for certification.
- Scheduling certification tests and demonstrations.
- Communicating with applicants on all matters pertaining to certification.
- Coordinating the make-up of technical teams (in collaboration with the national team).
- Maintaining records of certification panel meetings and decisions.
- Maintaining and publishing certification criteria and standards.
- Maintaining and publishing registers of certified and de-certified health information systems.
- Keeping track of re-certification audit reports and due dates.
- Maintaining a national database of county health information systems.
- Maintaining reports on Digital Health Solution certification outcomes.

The DHA will also:

- Maintain an inventory of all health information technologies in use within the country and maintain a public portal.
- Refer non-certified systems to national or regional labs for certification.
- Identify existing systems; advise system owners and vendors of certification requirements.
- Require new Digital Health Solution/vendor to provide proof of certification prior to implementation of their systems.
- Enforce the recommendations of the national certification team.
- Provide feedback to the national certification framework technical working group, based on challenges encountered during implementation.

- Support development, reviewing, and updating of standards certification framework's governance structure is intended to function seamlessly with the two levels of government to facilitate the objectives of the Digital Health Solutions~~HIS certification process~~ implementation.~~.~~ ~~A national body (the National Certification Panel) and designated county bodies (county health management teams, or CHMTs) The National Digital Agency~~shall be instituted to work together to publish and enforce the certification framework.

~~The National Certification Panel shall be established by the Principal Secretary at the MoH, and be supported by a secretariat within the ministry's Health Informatics division. This body shall be charged with the responsibility of ensuring the certification framework is operational. Its mandate is to work with regulatory authorities in both the health care sector and the information systems domain to ensure compliance with the laws governing these two sectors. The National Certification Panel shall be responsible for the development, review, and update of standards and guidelines, in accordance with national and international guidelines and best practices. These standards and guidelines shall be reviewed and updated by technical working groups in the corresponding domains within the ministry.~~

~~The county bodies will be charged with sole responsibility for ensuring that health information systems deployed in the counties meet the minimum requirements established by the national panel, in order to ensure uniformity of standards across the country.~~

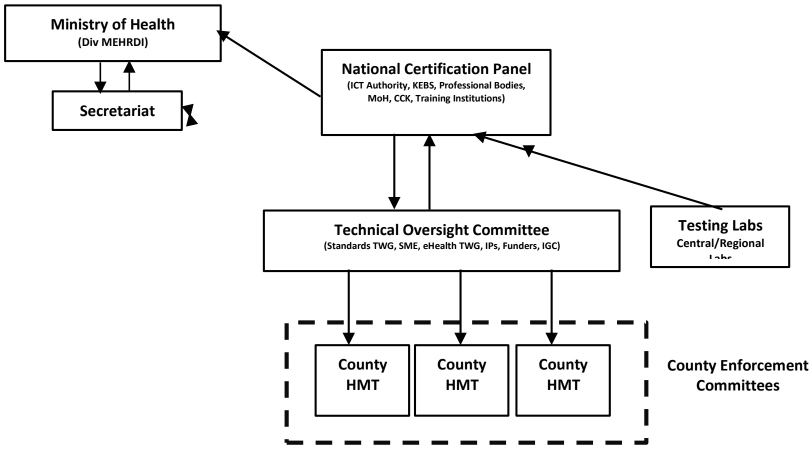

Ministry of Health
(Div MEHRDI)
Secretariat
National Certification Panel
(ICT Authority, KEBS, Professional Bodies, MoH, CCK, Training Institutions)
Technical Oversight Committee
(Standards TWG, SME, eHealth TWG, IPs, Funders, IGC)
Testing Labs
Central/Regional
Labs
County HMT
County HMT
County HMT
County Enforcement Committees

Figure 1. Certification governance structure.

2.2.1.1 National Certification Panel

The **National Certification Panel** is the oversight body in the certification structure. It is made up of representatives from the Ministry of Health's HIS and e-health departments, health sector regulatory bodies, the Kenya Bureau of Standards (KEBS), the ICT Authority (ICTA), professional associations, consumer representatives, and an Intergovernmental Council representative, as well as a legal representative from the MoH. The committee shall be domiciled within the Ministry of Health's Division of Health Informatics, Monitoring and Evaluation. The roles of this panel shall be to:

- Provide oversight of the standards development and certification process.
- Review, authorise, and publish HIS standards and guidelines.
- Review and authorise the drafting of new standards, and modifications or revisions to existing standards.
- Disseminate standards and guidelines, and the certification framework.
- Develop test methodologies, test data, and scripts.
- Review and revise test methodologies and plans.
- Provide arbitration services on contentious issues.
- Review and improve the certification framework every three (3) years.

2.2.1.2 Certification Committee

The National Certification Panel shall seat a **Certification Committee**, whose responsibility will be to review technical and documentation reports, and vote on whether or not to certify a system. This committee shall consist of experts in the domain or subject matter relevant to the area in which Digital Health Solution/Intervention~~HIS~~ certification is being sought. The role of the committee shall be to provide guidance on whether or not certification should be granted. The committee shall be convened on an as-needed basis; membership may change according to the technical expertise required during the review and certification process.

2.2.1.3 Testing Labs

The ~~National Certification Panel~~ DHA shall collaborate with relevant institutions of ~~higher learning~~ to set up and certify laboratory-based testing environments for the purpose of assessing digital health solutions ~~HIS~~ conformance with established criteria. These labs shall be set up in locations throughout the country, to ensure they are accessible by all potential applicants. ~~(Initial certification testing will take place at the Jomo Kenyatta University of Agriculture and Technology's (JKUAT) interoperability lab, which will be configured for that purpose.)~~ The specific functions of these testing labs will be to:

- Perform ~~Assist in the development of~~ tests ~~test scripts and methodologies~~ based on the DHA guidelines.
- ~~Perform objective HIS testing.~~
- Provide technical reports on testing to aid in certification decision-making.
- Provide a testing environment for development of standards and criteria.
- Assist with technical input on standardisation.
- Assist with field testing or demonstrations of existing digital health solutions/interventions~~facility-based systems~~.

2.2.1.4 Office of the Director General ~~Minsitryb~~~~**MoH Secretariat (Div MEHRDI**~~**)**

~~The **MoH secretariat** shall be based at the MoH offices; it shall be the coordinating body supporting the certification panel on administrative functions.~~ The DG- shall delegate to the directorate responsible of digital health and informatics~~be responsible~~ the functions of ~~for~~ development of policies, standards, and guidelines for ~~coordinating the~~ certification process, ~~including:~~

- ~~Receiving and reviewing applications for certification.~~
- ~~Scheduling certification tests and demonstrations.~~
- ~~Communicating with applicants on all matters pertaining to certification.~~
- ~~Coordinating the make-up of technical teams (in collaboration with the national team).~~
- ~~Maintaining records of certification panel meetings and decisions.~~
- ~~Maintaining and publishing certification criteria and standards.~~
- ~~Maintaining and publishing registers of certified and de-certified heath information systems.~~
- ~~Keeping track of re-certification audit reports and due dates.~~
- ~~Maintaining a database of county health information systems.~~
- ~~Maintaining reports on HIS certification outcomes.~~

~~2.2.1.15~~2.2.1.5 ~~County Health Management Team~~County Digital Health Committee

In each county, the ~~**County Health Management Team** (CHMT)~~ County Digital Health Committee (CDHC)will be tasked with enforcing the certification framework. Given their strategic locations within the counties, each CDHC~~CHMT~~ will be responsible for ensuring that only certified DHS/Is ~~health information systems~~ are in operation in their county's health sector. As part of their regulatory functions within the governance structure, the CDHC~~CHMTs~~ will perform spot checks to assess compliance; they shall inspect and review systems, and make recommendations regarding DHS/I~~HIS~~ de-certification or re-certification to the national committee. They shall also ensure that systems being implemented within the county health sector have been certified and registered by the MoH *before* allowing them to apply for certification to operate within the county. The committee will consist of; the county DPO, County ICT, County HRIO, DHA county representative, and a representative of the CEC, COH, CDH, and D. Medical Services~~Each team shall consist of the designated membership, including the County Health Records Officer (CHRIO), County Director of Health, Chief Nursing Officer, and ICT department representative.~~ Each team shall be charged with the responsibility to:

- Maintain an inventory of all health information technologies in use within the county.
- Refer non-certified systems to national or regional labs for certification.
- Identify existing systems; advise system owners and vendors of certification requirements.
- Require new Digital health Solution provider entrants to provide proof of certification prior to implementation of their systems.
- Enforce the recommendations of the national certification team.
- Provide feedback to the national certification framework technical working group, based on challenges encountered during implementation.

2.3 Certification Process

This section defines the processes a Digital Health Solution/Intervention~~health information system~~ must undergo to achieve certification. The test procedures are developed directly from the type of DHS/I criteria; every type of DHS/Icriterion/functionality must have a test procedure associated with it so that implementation of each requirement can be verified. The Digital Health Agency will develop the functionality tests for each type of the Digital Health Solutions and Interventions. The Ministry oOf Health will develop Standards and Guidelines for each type of DHS/I.

Each Digital Health Solution/Intervention~~HIS~~ being considered for certification must pass through six~~fou~~r stages:

- Self-Attestation and Application
- Document Review
- Scheduling and Testing
- Certification~~ and~~
- ~~Maintaining~~ Re-Certification & Ad Hoc audits
- Appeals

Commented [13]: Include section of revocation of certificate by DHA, and retracting access to the HIE - as part of its oversight function on DHS that have been certified:
This occurs in situations for example when a vendor is frustrating a county/ user/ hospital with downtime, poor support(help desk support), frequent security breaches etc

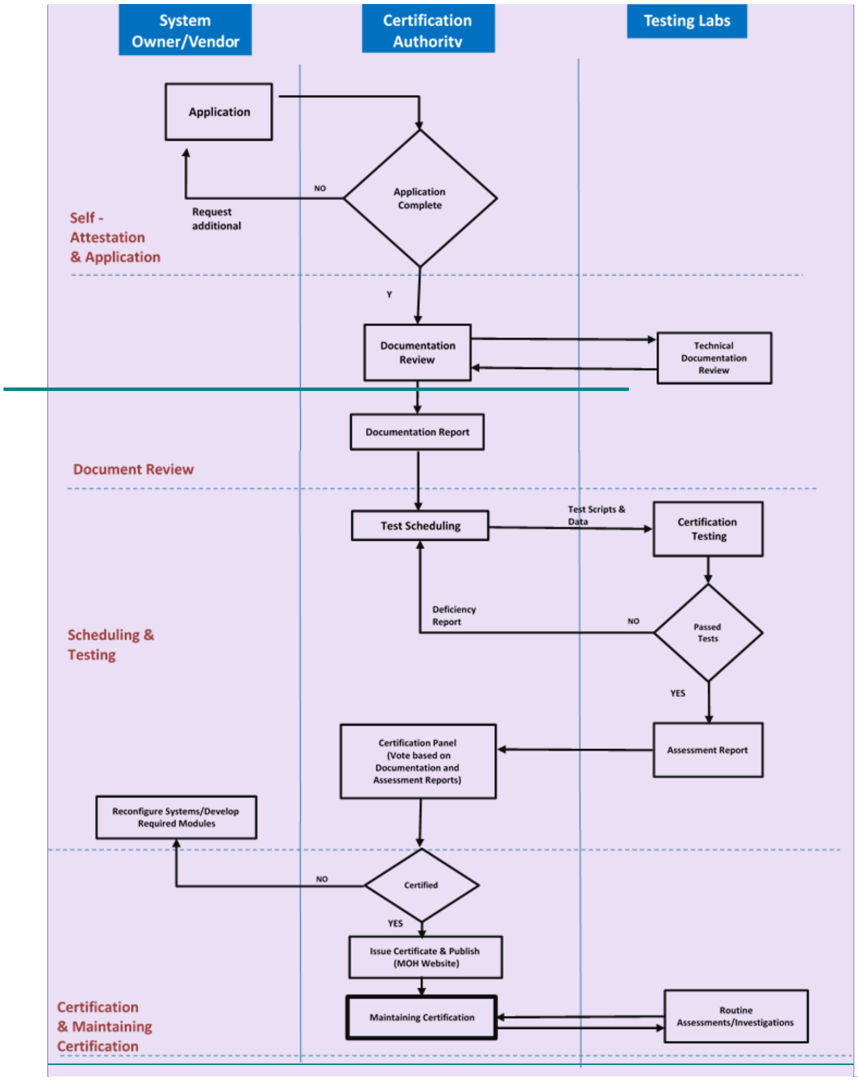

System Owner/Vendor
Certification Authority
Testing Labs
Application
NO
Application Complete
Request additional
Self - Attestation & Application
Y
Documentation Review
Technical Documentation Review
Documentation Report
Document Review
Test Scheduling
Test Scripts & Data
Certification Testing
Deficiency Report
NO
Passed Tests
Scheduling & Testing
YES
Certification Panel (Vote based on Documentation and Assessment Reports)
Assessment Report
Reconfigure Systems/Develop Required Modules
NO
Certified
YES
Issue Certificate & Publish (MOH Website)
Maintaining Certification
Routine Assessments/Investigations
Certification & Maintaining Certification

Figure 2. A logical flow diagram of the certification process

Commented [14]: Review this flow diagram @woghera@yahoo.com to include the re-certification process
Assigned to woghera

2.3.1 Self-Attestation and Application

The objective of this process is to encourage and facilitate the development and availability of Digital Health Solution/Intervention~~health information systems~~ that meet the minimum requirements set by the MoH. The certification process is for all digital health solutions in Kenya.~~the same in each county, regardless of the certification body (CB).~~

Prior to applying for certification, each Digital Health Solution~~vendor~~ should undergo a self-attestation procedure to ensure their system conforms to the applicable requirements and is ready for certification. The self-attestation process is intended to help ~~categorizecategorise~~ the Digital Health Solution/Intervention provider~~HIS system~~~~determine the minimum, thereby determining~~ w~~hich set of~~ identify the minimum compliance tests expected for certification~~should be performed~~.

An interactive, web-based self-attestation tool shall be provided by ~~through the~~ ~~MoH~~ Digital Health Agency~~Solution/Intervention~~~~HIS~~ certification web portal (Insert link). This tool will be for ~~e developed by a team of experts from the technical labs and systems domains, to ensure the establishment of comprehensive selection criteria for~~ determining which systems can proceed to the next stage of the process. The purpose here is to ensure that only those systems that qualify for certification testing make it to the application stage.

In addition to self-attestation, the Digital Health Solution developer ~~vendor~~ should be sure to review the standards & guidelines, certification requirements, and become familiar with them before submitting the application.

Submission of the application with the relevant product documentation will enable the Digital Health Agency ~~certification body (CB)~~ to fully understand the scope of the Digital Health Solutions ~~HIS~~ operations and functionalities. The DHA will prescribe all the requirements to be fulfilled for certification to begin.

~~The application also becomes the basis of the contract between the CB and the vendor or developer; it is critical for calculating how long the certification process will take, and determining the proper assignment of expertise in the appropriate functionality categories.~~

F~~ollowing acceptance of the application, the DCB contacts the vendor to schedule a mutually acceptable date for certificatio~~n. Certification ~~(or re-certification)~~ must take place within thirty (30) working days; however, within these limits, the certification audit can be scheduled on a date that suits both the Digital Health Solution developer ~~vendor~~ and DHA~~CB~~.

2.3.2 Documentation Review

The DHS/I developer will in submitting for certification, provide the following documentation for review;

- Corporation certificates/ identifying documents
- System manual and requirement specification
- Evidence of registration with the ODPC as a Processor and controller
- Data Protection Impact Assessment Report
- Security, privacy, and confidentiality Policy
- System back-up and recovery policy

The DHA will review this documentation and if satisfactory, the DHS will move to the next stage of certification.

Commented [15]: Include a sections which speaks to transition of existing digital health solutions to comply to the certification framework

Commented [16]: In this section, ensure to include a provision for the DHS that do not meet the requirements, time for this solutions to conform before a second review...

Formatted: Font: (Default) Arial, 11 pt, Font color: Black

~~2.3.2~~2.3.3Certification Testing/Audits

All Digital Health Solutions~~health information system~~s must undergo an audit. The purpose of this audit is to determine how well a digital health interventions/solution adheres to the following:

- Functionality
- Reporting and Alerts
- Security, Privacy, and Confidentiality
- Information Exchange and Interoperability

Formatted: Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.25" + Indent at: 0.5"

~~how well a system identifies and implements the minimum required functionality, and complies with applicable requirements or standards.~~ The DHA~~CB~~ will check to ensure the submitted documentation, demonstrations, Self-attestation results~~test results (if applicable)~~, and any other required supporting information demonstrate that the Digital Health Solution ~~HIS~~ meets the minimum requirements.

- The certification audits are non-consultative, which means that auditors are not permitted to instruct or advise the DHS owner~~vendor~~ on how to meet requirements while the audit is in progress.
- The auditors review the system against the certification requirements scoring tool.
- Any non-conformances observed during the audit are documented in the audit report.
- At the conclusion of the audit, the DHA will provide the DHS developer a certification testing/audit report to the developer ~~vendor is~~ informing~~inform~~ing~~ed~~ them of all observed non-conformances;

Formatted: Font color: Auto

- ~~only then are they informed or advi~~s~~ed as to the changes needed to meet the requirements.~~

2.3.4 Certification Decision and Issuance

~~2.3.3~~ Certification Decision and Issuance

Formatted: Normal, Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.25" + Indent at: 0.75", Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border)

To achieve certification, a DHS/I ~~system vendor~~ must meet the requirements for conformance established in the audit report.

- Each certification scheme has unique time-line requirements for conformance.
- The DHA~~CB~~ reviews the evidence submitted, and accepts corrective actions if they are sufficient to resolve the noted non-conformance.
- If the submitted corrective actions do not sufficiently resolve the non-conformance, the DHA~~CB~~ rejects them, and the vendor is required to re-submit within a specific time frame.
- ~~In particular cases, the DHACB can undertake a further site visit to verify corrective actions on non-conformances.~~
- The auditors do not decide certification. An independent team within the DHA~~CB~~ (not including any of the auditors) makes the final determination on certification, based on their review of the audit report and evidence of close-out of non-conformances.

- Only after a certification decision can a certificate be issued. The DHA~~CB~~ will notify the provider ~~vendor~~ in writing of the audit result.
- The DHA~~CB~~ will enter the DHS/I~~HIS~~ into the certification register, and issue a certificate to theprovider ~~vendor~~. The certification register will be published on the certification program's website, clearly indicating the areas of functionality for which the product has been certified.
- The entire process, from completion of the audit to issuance of the certificate of conformity, will take a maximum of~~typically takes about 45~~ 30 working days.

2.3.4 2.3.5 Re-certification & Ad Hoc Audits

To achieve recertification, the DHS/I developer is required to have maintained *all* certified functionalities and minimum requirements for a period of at least two (2) ~~hree (3)~~ years.During the implementation of the DHS/I the developer will ensure that they perform all the necessary updates and bug fixes to ensure they maintain certification conformity. ~~During the first phase of certification, system buyers and users will be guided by the MoH on contractual engagements with the system vendors to recommend a maintenance period that provides for system modifications and updates.~~

The DHA will in the period between the two years perform ad hoc audits to check for compliance and adherence to the certificate of conformity. Any reported case of breach of the certificate of conformity will lead to a fresh audit.

~~System owners are also expected to take necessary actions to sufficiently correct any non-conformances prior to re-certification.~~

Non-conformances may be the result of an audit, or of changes in standards and/or guidelines.

- For audits or investigations, the DHS/I~~vendor~~ is required to sufficiently correct the non-conformance issues raised, and prevent their recurrence. A certificate can be issued only when non-conformances have been appropriately addressed.
- For changes in standards or guidelines, the DHS/I~~vendor~~ shall be granted a specified grace period within which it~~the HIS~~ is expected to meet the designated criteria.
- ~~Periodically (every year or two), a certified vendor (a particular HIS) is required to submit to a re-certification audit in order to maintain certification.~~
- The re-certification audit will take place very close to the anniversary date of initial certification. Just as in the initial certification audits, the facility must address any non-conformances before certification will be issued.
- In particular cases, the DHA can undertake a further site visit to verify corrective actions on non-conformances.
- For system changes affecting security and interoperability, a fresh audit will be required
- All DHS will document change logs

Formatted: Font: (Default) Arial, 11 pt, Font color: Black

Formatted: Indent: Left: 0.75", No bullets or numbering

Commented [17]: Re certification and continuous auditing to be included here

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

- In case of system breaches, the DHS/I provider/user will notify the DHA on the nature of the breach and the solution implemented

~~In particular cases, the DHA can undertake a further site visit to verify corrective actions on non-conformances.~~

2.3.5 ~~Appeals~~ Review

The audit is a process of objectively evaluating health information systems for conformance or non-conformance to a specified standard. The auditors obtain objective evidence by observation, interviews, and review of documented records and test results. However, there may be occasions where DHS/I owner~~HIS~~ DHS developer ~~vendor~~s will not accept the outcomes of the audit, feeling that the auditors were either not objective, or did not adequately understand the process or technology or any other reasons. The DHS/I developer will submit an appeal form to the DHA~~A~~ is ~~All CBs performing HIS audits are~~ will~~required to have a complaints and appeals process in place to deal with such occasions. Where a vendor justifiably feels that the~~ DHA~~CB or its representative has been unfair in the process, they must first report it to the~~ DHA~~CB, and work through their complaints and appeals process.~~

The DHA will have an appeals committee with five (5) members that will review and make a decision on the appeal. These five will be nominated from the Digital Health Technical Working Group (TWG) ~~(do we need to specify non-DHA members??~~

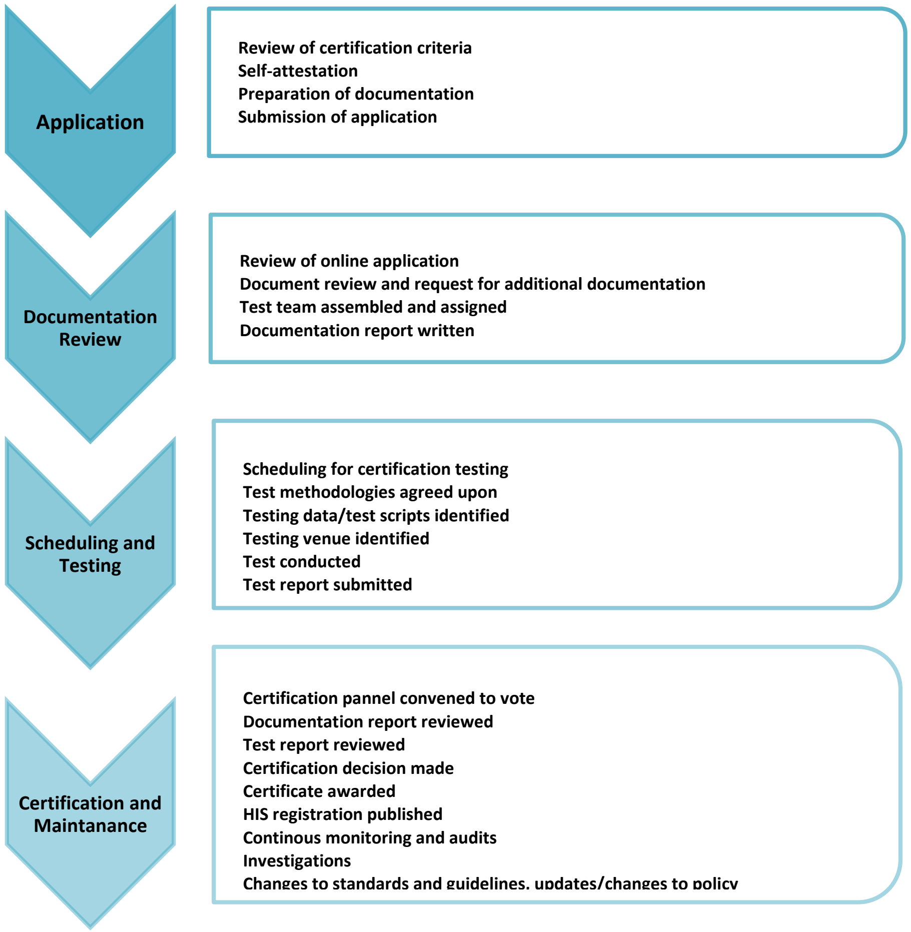
~~Appeals and/or complaints may also originate from users of the~~ DHS/I~~HIS. These are expected to be submitted through the Certification Authority, who then will initiate an investigation through the lab to verify the allegations in the complaint or appeal.~~

~~Rec~~

Formatted: Font color: Red

Formatted: Font: (Default) Arial, 11 pt, Font color: Black

Formatted: No bullets or numbering



Application

Review of certification criteria
Self-attestation
Preparation of documentation
Submission of application

Documentation Review

Review of online application
Document review and request for additional documentation
Test team assembled and assigned
Documentation report written

Scheduling and Testing

Scheduling for certification testing
Test methodologies agreed upon
Testing data/test scripts identified
Testing venue identified
Test conducted
Test report submitted

Certification and Maintanance

Certification pannel convened to vote
Documentation report reviewed
Test report reviewed
Certification decision made
Certificate awarded
HIS registration published
Continous monitoring and audits
Investigations
Changes to standards and guidelines, updates/changes to policy

Figure 3. Review of the certification process

Commented [18]: Table will need to be updated

2.3.6 Certification Criteria

	Certification Goal	Certification Aspects	Standards and Guidelines	Criteria Type (Required, Recommended, Optional)	System Type or Category
Functionality	**Demographics**	Ability to electronically record, change, and access patient demographic data in a standardised way including: 1. Sex/Gender 2. Date of birth 3. Residence details ~~Location~~ 4. Contact information; Phone number 5. Next of kin contact ~~5.~~6. Next of kin relation ~~6.~~7. ~~Ethnicity/preferred language~~ ~~7.~~8. ID Number/Passport/ Birth Certificate/Alien Number	Kenya DHS/I Standards and Guidelines	Required	All D soluti
	Computerised Provider Order Entry (CPOE)	Ability to electronically record, change, and access the following order types, at a minimum: - Medications - Dispensing - Laboratory - Radiology/Imaging - Physiotherapy - Occupation Therapy - Nutrition - Social Work - Counselling	Kenya DHS/I Standards and Guidelines	Required (Based on the solution)	EMR - mandatory

Formatted: Font color: Red

Formatted Table

Formatted: Font color: Red

Formatted: Font color: Red

		- Family Health History - Vital Signs - BMI and Growth Charts - Billing - MCH - Clinical Encounter			
	Problem List	Electronically record, change, and access a patient's active problem list in KENHDD ~~SNOMED CT® (or any other clinical vocabulary that has been mapped to SNOMED CT®)~~	Kenya DHS/I Standards and Guidelines KENHDD ~~KENHDD~~ ~~SNOMED CT®~~	Required	All DHS solutions
	HPT ~~**Medication/ Allergy List**~~	Electronically record, change, and access a patient's active prescribed HPT~~medication~~ list, as well as HPT~~medication~~ history: - HPT Registry ~~RxNorm~~ in instances where EHR technology would be used to perform external transmissions Electronically record, change, and access a patient's active HPT~~medication~~ allergy list, as well as HPT~~medication~~ allergy history - Encourage EHR technology developers to include capabilities that may go beyond certification requirements, particularly where that may improve patient safety - EHR technology natively records HPT~~medication~~ allergies directly into HPT Registry ~~RxNorm~~	~~Kenya National Pharmaceutical Policy (2008)~~ ~~Kenya Essential Medicines List (2010)~~ HPT Registry (PPB)	Required	EMR-Mandatory
	Allergy List	Electronically record, change, and access a patient's active allergy list, as well as medication allergy history	Non-HPT Allergies (Value sets)		EMR - Mandatory

Formatted: Font color: Red

		- Encourage EHR technology developers to include capabilities that may go beyond certification requirements, particularly where that may improve patient safety			
	Clinical Decision Support (CDS)	Evidence-based decision support interventions. Enable a limited set of identified users to select (i.e., activate) one or more electronic clinical decision support interventions based on each one plus at least one of the following data: - Problem list (KENHDD) - Medical list(HPT Registry) - HPT~~Medical~~ allergy list - Non-HPT allergy list - Demographics - Laboratory tests and values/results - Vital signs	HL7 Clinical Decision Support Kenya DHS/I Standards and Guidelines	Optional	EMR Optio
	Clinical Summary	Enable a user to create a clinical summary for a patient, in human-readable format and exchangeable via the Kenya HIE ~~formatted according to standards.~~ Minimum data elements: - Patient name - Sex - Date of birth - Provider's name and office contact information - Date and location and reason for visit - Problems - Referrals to other providers - Medication and medical allergies - Laboratory tests and results - Diagnostic tests pending and future schedule tests	~~HL7 Implementation Guide for CDA~~ ~~IHTSDO~~ ~~HCPCS and CPT~~ ~~SNOMED CT®~~ ~~ICT – 9, ICD - 10-PCS~~ ~~LOINC®~~ ~~RxNorm~~ Kenya Implementation Guide for FHIR	Required	All D Solut

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

		- Vital signs—height, weight, blood pressure, BMI - Procedures - Care Plan/Action taken; (i) Prevention. (ii) Diagnosis. (iii) Treatment. (iv) Management - Care team members			
	Electronic Prescribing	Electronically create prescriptions and prescription-related information for electronic transmission (including diagnostic test results, problem list, medication lists, medication allergies, discharge summary, procedures) upon request	RxNorm vocabulary standard NCPDP SCRIPT as the exchange standard		
	Clinical Quality Measures	- Capture—electronically record all of the data identified in the designated standard - Calculate—electronically calculate each and every clinical quality measure for which it is presented for certification - Import—electronically import a data file formatted in accordance with the designated standard - Export—electronically export a data file formatted in accordance with the designated standard - Electronic submission—electronically create a data file for transmission of clinical quality measurement data	~~HL7 Implementation~~ ~~Guide for CDA® -Quality Reporting Document Architecture~~ ~~Data Element Catalog~~ Kenya DHS/I Standards and Guidelines	Required	All D Solut
	~~Laboratory and Imaging~~	~~X-rays~~			
	~~Family Health History~~				
	~~Vital Signs, BMI and Growth Charts~~	~~Electronically capture and chart changes in the following vitals:~~ ~~(A) Height~~ ~~(B) Weight~~ ~~(C) Blood pressure~~			

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted: Pattern: Clear (Custom Color(RGB(182,215,168)))

Formatted ...

Commented [19]: Need to be worked on

Formatted ...

Formatted ...

Formatted ...

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Commented [20]: consider deleting this section

Formatted: Highlight

Formatted: Highlight

Commented [21]: Consider for deletion

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Space After: 0 pt

		~~(D) Calculate and display body mass index (BMI)~~ ~~(E) Plot and display growth charts for children 2–20 years, including BMI~~			
	~~**Drug Formulary**~~				
	Patient List Creation	**The system should be able to:** - **~~-~~schedule,** - **create a patient list,** - **make appointments and** - **send alerts**	Kenya DHS/I Standards and Guidelines	Optional	All DHS Solutions
	~~**Patient-Specific Educational Resources**~~				
	~~**Clinical Information Reconciliation**~~				
Reporting and Alerts	**Immediate Reportable Diseases**	**As per MOH Guidelines/ SOPs** ~~- AFP, VHF (ebola, Marburg), cholera, dengue, Guinea worm, measles, SARS,~~ ~~- MDR/XDR TB (lab-confirmed)~~ ~~- Yellow fever~~ ~~Plague~~ ~~System should be able to generate the IDSR weekly reports:~~ ~~Epidemic-prone diseases~~ ~~Diseases targeted for eradication/elimination~~ ~~Other major disease events of public-health importance~~ ~~Food poisoning, chemical event, collapsed building, massive death of animals, landslides~~ ~~Human influenza—new subtype~~ ~~SARS~~	Health Data Governance Framework	Required	All DHS solutions

Formatted: Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.25" + Indent at: 0.5"

Formatted Table

Formatted: Indent: Left: 0.5", No bullets or numbering

		~~- Smallpox~~ ~~Any other public health event of international concern~~ -			
	IDSR Reporting (Weekly)	~~System should be able to generate the IDSR weekly reports:~~ ~~- Epidemic-prone diseases~~ ~~- Diseases targeted for eradication/elimination~~ - ~~Other major disease events of public-health importance~~			
	Public Health Events	- ~~Food poisoning, chemical event, collapsed building, massive death of animals, landslides~~			
	Diseases or Events of International Concern	~~- Human influenza—new subtype~~ ~~- SARS~~ ~~- Smallpox~~ - ~~Any other public health event of international concern~~			
	Routine Health Reporting				
Data Exchange and Interoperability	**Data Transmission and Exchange**	View, download, and transmit information ~~between~~ as per Kenya National HIE to the Kenya National Core Digital Health Services~~:~~ ~~- Patient and provider~~ ~~- Provider and provider~~ ~~- Providers and public health agencies (immunisation registries, births and deaths)~~ - ~~Laboratory tests (X-rays, test results/values)~~	~~SNOMED CT~~ ~~ICD-10-CM~~ ~~RxNorm~~ ~~LOINC~~ ~~CVX - immunizations~~ Kenya Implementation Guide for FHIR	Required	All D Solut
	Interoperability	- Unstructured Data Exchange—the exchange of human-interpretable unstructured data, such as free text. - Structured Data Exchange—the exchange of human-interpretable structured data intended for manual and/or automated handling, but requiring manual compilation, receipt, and/or message dispatch. - Seamless Sharing of Data—involves the automated sharing of data amongst systems based on a common exchange model.			

Formatted: Font: (Default) Arial, 11 pt, Font color: Black

Formatted: Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border)

Formatted: Font: (Default) Arial, 11 pt, Font color: Black

Formatted: Space After: 0 pt, Line spacing: single, No bullets or numbering

Formatted: Space After: 0 pt, Line spacing: single, No bullets or numbering

Formatted: Font: (Default) Arial, 11 pt, Font color: Black

Formatted: Font: (Default) Arial, 11 pt, Font color: Black

Formatted: Space After: 0 pt, Line spacing: single, No bullets or numbering

Formatted: Indent: Left: 0", First line: 0", Line spacing: single

Formatted Table

		- Seamless Sharing of Information—the universal interpretation of information through data processing based on co-operating applications.			
~~y~~	**Security, Privacy, and Confidentiality**	Protect electronic health information created or maintained by the certified DHS/I~~HIS~~ through the implementation of appropriate technical capabilities. - Ensure the confidentiality, integrity, and availability of all electronic health information the system creates, receives, maintains, or transmits. - Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. - Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under law. o Authentication, access control, and authorization ▪ DHS/I unique identification & authentication, ▪ Authenticate Unique User ▪ Establish Permitted User Access o Auditable events and tamper resistance (audit trail and reports) o Version/Amendment tracking o Automatic log-off o Emergency access o Encryption of data at rest and data in transit~~Data, Storage & Device encryption~~ o Integrity ~~o~~- Conduct the Data Protection Impact Assessment ~~Secure messaging—Use secure electronic messaging to communicate with patients about relevant health information.~~	Data Protection Act, 2019 Digital Health Act, 2023 Health Act, 2017 ~~Kenya— Privacy and confidentiality guidelines,~~ ASTM Guidelines E2147-01 45 CFR part 11	Required	All DHS/I solutions

Formatted: Right: 0.09"

Formatted Table

Formatted

		~~- Encryption and hashing of electronic health information~~			

2.4 Testing Methods

The **scope of certification** identifies the specific tests or types of tests or capability for which the DHS/I~~HIS~~ is certified. The **objective of testing** is to establish whether or not the DHS/I~~HIS~~ complies with the requirements for certification, and can competently perform the tasks for which certification is sought. The test procedures are developed directly from the type of DHS/I ~~criteria;~~ every type of DHS/I~~criterion/~~functionality must have a test procedure associated with it so that implementation of each requirement can be verified. The Digital Health Agency will develop the functionality tests for each type of the Digital Health Solutions and Interventions. The Ministry o~~O~~f Health will develop Standards and Guidelines for each type of DHS/I.

~~There are several methods of testing available for a particular requirement, depending on type of implementation; it is the responsibility of the testing body to identify and clearly document the testing procedure beforehand. Procedures may change from time to time, as technology and standards change; it is the responsibility of the testing body to update them regularly, under the oversight of the certification authority. The following methodologies shall be used to test for compliance.~~

2.4.1 Self-Attestation

In the context of this framework, **self-attestation** refers to an approach that would allow a DHS/I developer ~~vendor~~, guided by a checklist of the minimum set of requirements, to make the claim that their DHS/I~~its HIS~~ is compliant with a reasonable level of confidence. This methodology is meant to guide the application process such that the vendor knows exactly what requirements their system would be tested against for compliance. The underlying premise supporting this methodology is that DHS/I developer~~HIS vendor~~s provide an honest attestation of their system, and are able to demonstrate it during testing. (Other vendors may provide documentation supporting compliance, but be unable to provide demonstration or attestation, and thus cannot show compliance.) The methodology also helps to identify the category to which the HIS belongs, and the appropriate tests required under that category.

Self-attestation is the initial step in certification testing. The process will result in recommendations as to which documentation should be submitted with the application for certification.

2.4.2 Document Review

After the self-attestation process is complete, and the vendor is confident that they can apply for certification, the next step is to submit the required documentation, based on the recommendations given during the self-attestation process. This includes any certificates required to accompany the application documents. The document copies are scanned and submitted electronically to the secretariat for vetting. The original and/or physical documents must also be presented during testing for validation.

The applicant must also be able to show that they meet the certification requirements of other relevant government agencies. For example, if approval by the Information and Communications Technology (ICT) Authority or any other institution is also required, such approval must be presented at this stage. Submitted documentation shall be reviewed by the secretariat, officially kicking off the certification process.

The purpose of this step is to ensure that the certification process takes into account any existing regulations and guidelines pertaining to implementation of ICT systems. In the event that certain documentation is missing, the secretariat will co-operate with the applicant to ensure that all relevant documentation is available before initiating the certification process. A documentation report shall then be filed; it will form part of the final evaluation for certification.

2.4.3 Demonstrations/Test Labs

Demonstration tests are directed at evaluating the conformance of a health information system to specified standards and criteria; this should not be confused with demonstration of a system's capabilities. The result of such a demonstration is therefore a decision to whether or not to certify the HIS. Demonstrations shall be guided by test scenarios or scripts, with specific output goals defined and published by the testing body. This, however, can change should the testing body deem it necessary.

Demonstration testing may be conducted as projected presentations, or as field tests. But, to be effective, they must:

- Use test scripts or scenarios that have been reviewed, and accepted as representative of the minimum requirements (and thus be of fixed-build standard throughout testing).
- Represent, as closely as practicable, typical operational use of the HIS.
- Provide sufficient test observations to produce results that are satisfactory, or can be replicated using another method.

If any of these conditions cannot be fulfilled, the HIS will be deemed as not meeting the minimum requirements for this testing methodology—and thus non-compliant.

2.4.4 Field Testing

This refers to a methodology that applies *only* to existing or currently operating systems seeking certification. It involves performing the assessment and/or tests on site (i.e., on the premises where the HIS is operational), or in a setting that allows for a full review of system requirements. This shall be performed under one of two categories:

a. The testing body goes to the field site, and performs the assessment in the operating environment.
b. The vendor runs a duplicate platform in a test environment that simulates the actual operating environment (to avoid service disruptions in the operational setting).

The conditions for the choice and method for performing this type of test must be agreed on in advance by the testing body and the vendor.

2.4.5 Full Testing

In this approach, every aspect of the HIS is tested to determine whether or not it meets the designated standards and requirements. This applies only to systems that the vendor feels have fully met the certification requirements for each and every category. Although the phased/modular approach is recommended, it is the prerogative of the vendor to decide whether or not they want to do a complete or full test. In this instance, the vendor would have to apply for full testing of the HIS, and to suggest that the system meet all criteria stipulated by the framework. Assuming the testing procedures are adequate, this provides the highest possible level of assurance that the product fully conforms to certification standards. It is the most expensive and time-consuming testing approach, but is encouraged for fully customized products.

2.4.6 Investigations

This method applies to systems already in use, as well as to certified systems that experience alleged failures during actual use, and are under investigation to determine the cause(s) of failure/non-compliance for the purpose of suggesting appropriate corrective action.

This certification framework will rely on two or more of the above methods during the certification process. Choice of method will depend on the vendor, and the designated standards for the criteria under which testing will be done. The choice of method can greatly affect both the cost of the certification program and the level of confidence ascribed to it. During the assessment, deficiencies may be identified. A deficiency is any non-conformity to certification requirements, including:

a) The inability of a system to perform a test, or type of test, for which certification is sought.
b) The HIS does not conform to a standard/criterion, is not adequately documented, or is not completely implemented in accordance with the documentation provided.

Commented [22]: This section has been repeated